ORDER, RANDOMNESS AND ORBIT DISTRIBUTIONS FOR DYNAMICS OF BIRATIONAL MAPS OVER FINITE FIELDS

A thesis submitted for the degree of

Doctor of Philosophy

By

Timothy Chap-On Siu

Supervisor: Professor John A G Roberts

School of Mathematics and Statistics,

UNSW Sydney

August 2019

Thesis/Dissertation Sheet

Surname/Family Name	:	**SIU**
Given Name/s	:	**Timothy Chap-On**
Abbreviation for degree as give in the University calendar	:	**PhD**
Faculty	:	**Faculty of Science**
School	:	**School of Mathematics and Statistics**
Thesis Title	:	**Order, randomness and orbit distributions for dynamics of birational maps over finite fields**

Abstract 350 words maximum: (PLEASE TYPE)

We consider birational maps in affine space of two or more dimensions over finite fields. We see that when we look at the mappings modulo p, we lose all topology and sense of "closeness" of points that is present over the real or complex numbers. However, algebraic properties such as the presence of a reversing symmetry (reversible maps) or preserving an invariant algebraic surface (integrable maps) also reduce algebraically to the finite field. For birational maps on the finite field, we have the possibility of periodic orbits or singular orbits. We investigate how these algebraic properties manifest themselves in the orbits and show how random (i.e. probabilistic) models tailored for these properties can be used to predict various statistics of the orbits such as the number of periodic orbits, the number of periodic points and the distribution of the lengths of the orbits. Furthermore, this can be used as a diagnostic for whether a given mapping possesses such properties. We see that these properties alone seem to be the constraining property for many of the statistics of the dynamical system, and not the details of the map itself. We provide in-depth analysis and numerical studies on a few representative examples and also show the efficacy of these ideas on a menagerie of maps from the literature.

FOR OFFICE USE ONLY Date of completion of requirements for Award:

ORIGINALITY STATEMENT

'I hereby declare that this submission is my own work and to the best of my knowledge it contains no materials previously published or written by another person, or substantial proportions of material which have been accepted for the award of any other degree or diploma at UNSW or any other educational institution, except where due acknowledgement is made in the thesis. Any contribution made to the research by others, with whom I have worked at UNSW or elsewhere, is explicitly acknowledged in the thesis. I also declare that the intellectual content of this thesis is the product of my own work, except to the extent that assistance from others in the project's design and conception or in style, presentation and linguistic expression is acknowledged.'

Signed ……..

Date ……..

INCLUSION OF PUBLICATIONS STATEMENT

UNSW is supportive of candidates publishing their research results during their candidature as detailed in the UNSW Thesis Examination Procedure.

Publications can be used in their thesis in lieu of a Chapter if:

- The student contributed greater than 50% of the content in the publication and is the "primary author", ie. the student was responsible primarily for the planning, execution and preparation of the work for publication
- The student has approval to include the publication in their thesis in lieu of a Chapter from their supervisor and Postgraduate Coordinator.
- The publication is not subject to any obligations or contractual agreements with a third party that would constrain its inclusion in the thesis

Please indicate whether this thesis contains published material or not.

☐ *This thesis contains no publications, either published or submitted for publication (if this box is checked, you may delete all the material on page 2)*

☐ *Some of the work described in this thesis has been published and it has been documented in the relevant Chapters with acknowledgement (if this box is checked, you may delete all the material on page 2)*

☐ *This thesis has publications (either published or submitted for publication) incorporated into it in lieu of a chapter and the details are presented below*

CANDIDATE'S DECLARATION

I declare that:

- I have complied with the Thesis Examination Procedure
- where I have used a publication in lieu of a Chapter, the listed publication(s) below meet(s) the requirements to be included in the thesis.

Name	Signature	Date (dd/mm/yy)

Postgraduate Coordinator's Declaration (to be filled in where publications are used in lieu of Chapters)

I declare that:

- the information below is accurate
- where listed publication(s) have been used in lieu of Chapter(s), their use complies with the Thesis Examination Procedure
- the minimum requirements for the format of the thesis have been met.

PGC's Name	PGC's Signature	Date (dd/mm/yy)

Abstract

We consider birational maps in affine space of two or more dimensions over finite fields. We see that when we look at the mappings modulo p, we lose all topology and sense of "closeness" of points that is present over the real or complex numbers. However, algebraic properties such as the presence of a reversing symmetry (reversible maps) or preserving an invariant algebraic surface (integrable maps) also reduce algebraically to the finite field. For birational maps on the finite field, we have the possibility of periodic orbits or singular orbits. We investigate how these algebraic properties manifest themselves in the orbits and show how random (i.e. probabilistic) models tailored for these properties can be used to predict various statistics of the orbits such as the number of periodic orbits, the number of periodic points and the distribution of the lengths of the orbits. Furthermore, this can be used as a diagnostic for whether a given mapping possesses such properties. We see that these properties alone seem to be the constraining property for many of the statistics of the dynamical system, and not the details of the map itself. We provide in-depth analysis and numerical studies on a few representative examples and also show the efficacy of these ideas on a menagerie of maps from the literature.

Acknowledgements

I would first like to thank my supervisor, John Roberts, who encouraged me from the beginning to undertake this research work and has guided and supported me in every way for all these years.

I am also grateful to all my friends and family who have sustained me during this time.

Contents

Chapter 1

Introduction

In this thesis, we investigate the dynamics of birational (invertible rational) maps on affine space reduced to the finite field. By studying maps on a finite field, we can describe the dynamics completely by performing a full orbit decomposition, that is, finding the orbit length of every point by direct computation (for small finite fields at least). The main dynamical questions relate to orbit statistics: their number, length and distribution. We are interested in studying the mathematical structure underpinning these statistics. For polynomial automorphisms (invertible polynomial maps) over finite fields, all orbits will be periodic cycles. A motivating question is whether there are classes of maps with similar cycle structures or if we can find the average or expected statistics for classes of maps.

For example, a polynomial automorphism over the finite field $\mathbb{F}_p$ in d dimensions has p^d points and is a realisation of a permutation over the same number of points. Thus, a good analogy to this problem may be obtained by looking at the symmetric group S_n, the set of permutations on n points. There are many questions we can ask about the cycle structure of a permutation. What is the expected length of the longest cycle? How many cycles do we expect of length k? What is the expected number of cycles? What is the distribution of the number of cycles? The simplest non-trivial examples are linear maps in two dimensions commonly known as cat maps which over the finite space $\mathbb{F}_p^2$ can be written as

$$\begin{aligned} x' &= \alpha x - y \\ y' &= x, \end{aligned} \tag{1.1}$$

where each coordinate is taken modulo p and parameter $\alpha \in \mathbb{F}_p$. This map preserves the conic section given by

$$I(x, y) = x^2 - \alpha xy + y^2 \tag{1.2}$$

since $I(x', y') = I(x, y)$. We say that $I(x, y)$ is an *integral* for the map (1.1). Percival and Vivaldi [55] showed that in almost all cases, all orbits have the same cycle length which is a divisor of $p + 1$ or $p - 1$. A more interesting example can be found by looking at non-linear polynomial automorphisms. For example, take the classical Hénon quadratic family [29] over $\mathbb{F}_p^2$,

$$\begin{aligned} x' &= y, \\ y' &= -\delta x + y^2 + \epsilon \end{aligned} \tag{1.3}$$

with integer parameters $\delta \neq 0, \epsilon$. For $\delta = 1$, the map has the property called *reversibility*, and can be written as the composition of two involutions. This gives the map a reversing symmetry, and orbits can be classified as symmetric or asymmetric (see chapter 5). In 2005, Roberts and Vivaldi [63] conjectured that the scaled distribution of the large prime length symmetric orbits for reversible polynomial automorphisms (such as (1.3)) is asymptotically the same as the distribution of all orbit lengths, which is independent of the map and given by

$$\mathcal{R}(x) := 1 - e^{-x}(1 + x). \tag{1.4}$$

Here the scaled distribution $\mathcal{D}_p(x)$ for $\mathbb{F}_p^2$ refers to

$$\mathcal{D}_p(x) = \frac{\#\{z \in \mathbb{F}_p^2 \mid t(z) \leq \kappa x\}}{p^2}, \tag{1.5}$$

where κ is a scaling parameter and $t(z)$ is the length of the orbit of z. Furthermore, for these reversible maps we can obtain a good estimate for the number of orbits by looking at the reversing symmetries (without calculating any dynamics). In contrast, for non-reversible maps (for example for parameters $\delta \neq 1, 0$ in (1.3)), Roberts and Vivaldi [63] conjectured that the limiting distribution is the same as for a random permutation, $\mathcal{I}(x) = x$. They also observed that the length of the longest orbit was consistent with the expected length for a random permutation [25]. Intuitively, this says that a map with no symmetries or other constraining structure will behave like a random permutation, while reversible maps obey a different universal distribution $\mathcal{R}(x)$. They investigated

this further in [64], by considering the composition of random involutions by using a combinatorial model, showing that the expected limiting distribution of the orbit lengths (with mild restrictions on the size of their fixed sets) was indeed $\mathcal{R}(x)$.

A large part of the work in this thesis is motivated by and can be seen as an extension the works of Roberts and Vivaldi [62, 63, 64] of studying maps over finite fields. They used this idea to detect signatures of two algebraic properties: having an integral or being reversible. Their work was concerned mainly with the length of orbits or the distribution of the lengths, while in this thesis we put a larger focus on the number of orbits. We will see that this is an effective discriminator for these two algebraic properties, even for higher dimensional maps. There is much interest in detecting integrals in discrete systems. In particular, the area of discrete integrable systems is a very active research area. For a review of several integrability tests, see [27] and references therein. We will see how the ideas for polynomial automorphisms can help us to study the more general case of birational maps (invertible rational maps) which have singularities where the action of the map is undefined.

In chapter 2, we introduce basic definitions related to mappings over a finite field and briefly describe related literature in this area such as the study of permutation polynomials, random permutations and random maps. The enumeration of the number, lengths and distribution of orbits for higher dimensional maps on the finite field was only recently considered by Roberts and Vivaldi in [62, 63, 64]. In chapter 3, we review some results on the orbit statistics of random permutations. We compare these to the (dissipative) Hénon map (1.3), a representative polynomial automorphism in two dimensions, and see that its orbit statistics are well modelled by those of a random permutation. In chapter 4, we extend the random permutation to allow for singular points. We call these s-permutations, where s is the number of singular points and $s = 0$ corresponds to the case of a permutation in chapter 3. We see the distribution $\mathcal{R}(x)$ manifest itself in the distribution of the lengths of singular orbits for s-permutations. We provide exact expected values in the enumeration of the periodic orbits and points. We compare this to various birational maps in two dimensions and see that these are well modelled by s-permutations.

In chapter 5, we introduce the algebraic property of reversibility and show the effect of the reversing symmetries on the dynamics of the map reduced to the finite field. In chapter 6, we introduce the algebraic property of an integral of motion showing its effects on the

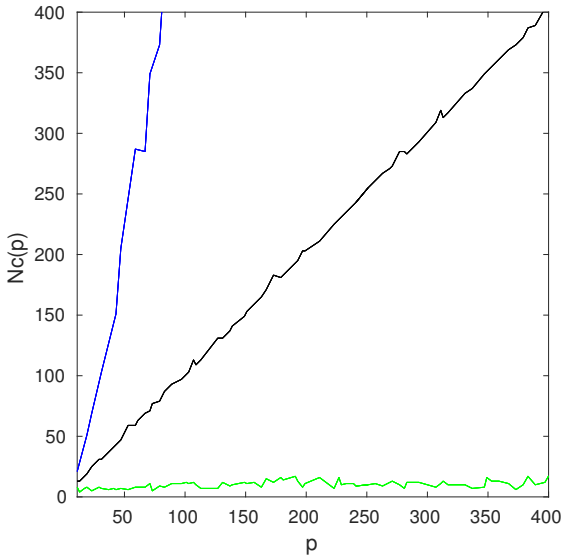


Figure 1.1: Maps over finite fields $\mathbb{F}_p$: growth of the number of cycles with prime p for an integrable map (top), a non-integrable reversible map (middle), and a non-integrable, non reversible map (bottom).

orbits. We consider in detail the cat map 1.1, a linear mapping in two dimensions reduced to the finite field providing results on its orbit decomposition. We also study a family of QRT maps, summarising results in [33] and adding some further observations. In chapter 7 we study the piecewise cat map, first studied by Lagarias and Rains [37, 38, 39] over the real plane. We consider the map reduced to the finite field, where we also parameterise the position of the transition in the piecewise function, which we call the "switch". We study the distribution of the orbits, and see that it seems to have limiting distribution $\mathcal{R}(x)$. By varying the "switch", we see the departure from the orbit length distribution of the cat map from Percival and Vivaldi [55] to $\mathcal{R}(x)$.

In chapter 8, we revisit the combinatorial model in [64]. We extend the model to allow for singular points, but also shift our attention to the number of asymmetric orbits, which was not previously considered. In chapter 9, we develop a practical test for the number of rational integrals in a reversible map by using the models for the number of asymmetric periodic orbits. In [63], various statistics of maps were compared in the finite space $\mathbb{F}_p^2$. For example, the number of cycles for integrable maps, non-integrable R-reversible map and a non-integrable non-R-reversible map were conjectured to be asymptotic to $p \log p, p$ and $2 \log p$ respectively. This is shown in figure 1.1. Roberts and Vivaldi [62] proposed a method to detect integrals in 2D by considering the maximum orbit lengths of orbits when reduced to the finite field. This utilised the Hasse-Weil bound and was shown to

be very effective, even for separating near-integrability from genuine integrability for 2D maps. In chapter 9 we investigate the idea of using orbit statistics for detecting integrals in higher dimensions. We will see that the method used in [62] is only effective as a test of super-integrability (when the number of integrals is one less than the dimension of the space). We propose a new method using the statistic of the number of asymmetric periodic orbits. This uses the results from chapter 8 that provide a heuristic for how this number changes for reversible maps with integrals. We test our model against a large number of integrable maps in the literature and provide data showing the efficacy of this method.

1.1 Original research contributions

This thesis aims at presenting the results of my research during my PhD. Here I will outline the major contributions contained in this thesis. In order of appearance, they are:

1. A combinatorial model for maps with singularities which is effective in estimating various statistics of birational maps (Chapter 4).
2. Analysis of the cycles of a Piece-wise linear map showing the departure from a singular distribution to $\mathcal{R}(x)$ (Chapter 7).
3. Extension of the combinatorial model in [64] of the composition of two involutions on a finite space to allow for singularities and providing asymptotic values for various statistics, but in particular focussing on asymmetric cycles which was not previously considered (Chapter 8).
4. A new method for testing the number of rational integrals in reversible maps using a numerical test on the number of asymmetric cycles (Chapter 9).

Chapter 2

Maps and dynamics over finite fields

This chapter introduces maps and (discrete) dynamical systems and gives a brief overview of some history and the current state of some results in dynamical systems. We focus on finite dynamical systems as this is what we are mainly concerned with in this thesis.

2.1 Polynomial and rational maps

Definition 2.1.1. Let K be a field. A mapping over the d-dimensional affine space K^d is a function $L : K^d \to K^d$. This takes a point $\mathbf{x} = (x_1, \ldots, x_d) \in K^d$ to $\mathbf{x}' = (x_1', \ldots, x_d') \in K^d$ via

$$\begin{aligned} L : x_1' &= f_1(x_1, \ldots, x_d) \\ x_2' &= f_2(x_1, \ldots, x_d) \\ &\vdots \\ x_d' &= f_d(x_1, \ldots, x_d), \end{aligned} \tag{2.1}$$

where each f_i is a function $f_i : K^d \to K$. Alternatively, more compactly, we can also write

$$L : \mathbf{x}' = F(\mathbf{x}), \tag{2.2}$$

where $F = (f_1, f_2, \ldots, f_d)^T$.

With K a field, firstly consider polynomials $f_1, f_2, \ldots, f_d \in K[x_1, x_2, \ldots, x_d]$. Then L is a *polynomial map* over K^d. We also consider the case when $f_1, f_2, \ldots, f_d$ are rational

functions. That is, for $1 \leq i \leq d$ we can write $f_i = g_i/h_i$ where $g_i, h_i \in K[x_1, x_2, \ldots, x_d]$, that is,

$$f_i(x_1, x_2, \ldots, x_d) = \frac{g_i(x_1, x_2, \ldots, x_d)}{h_i(x_1, x_2, \ldots, x_d)}. \tag{2.3}$$

We will assume that g_i and h_i are coprime. One problem is that these rational functions f_i now may not be functions. The f_i's will be defined at all $\mathbf{x} \in K^d$ where $h_i(\mathbf{x}) \neq 0$ and, in this case, the mapping L is defined at $\mathbf{x}$ where $f_i(\mathbf{x})$ in (2.1) is defined for all $1 \leq i \leq d$. The largest set for which L is defined is the domain of L. Its complement is called the locus of indeterminacy which we denote as $\mathrm{Sing}(L)$. It is where L is not defined, that is,

$$\mathrm{Sing}(L) = \{\mathbf{x} \in K^d \mid h_i(\mathbf{x}) = 0 \text{ for some } i = 1, 2, \ldots, d\}. \tag{2.4}$$

We will call $\mathbf{x} \in \mathrm{Sing}(L)$ a *singular point* of L. Thus L is a *rational map* with domain $K^d - \mathrm{Sing}(L)$.

2.2 Discrete dynamical systems

The core motivation for studying maps is that they can be used to model a variety of phenomena. A dynamical system on a space S is a map $L : S \to S$ where we study the action of L on points in S, namely for $z \in S$ we consider

$$z' = Lz, \tag{2.5}$$

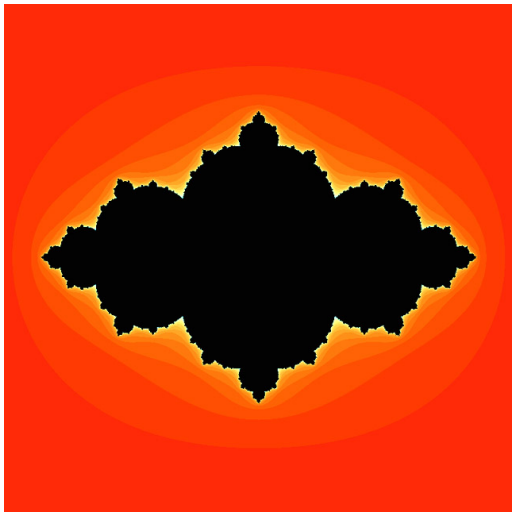
where z' denotes the next iterate of z under the mapping L.

Definition 2.2.1. The (forward) orbit of a point $z \in S$ is given by the set

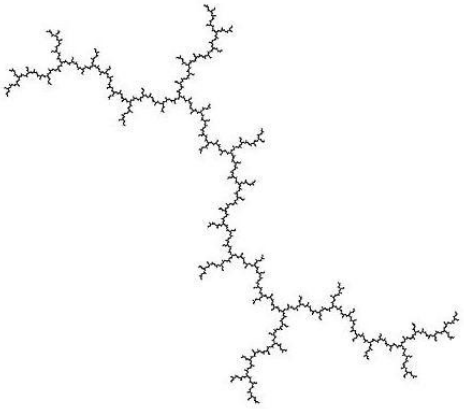
$$\begin{aligned} \sigma(z) &= \{L^k z \mid k \in \mathbb{N}\} \\ &= \{z, Lz, L^2 z, \ldots\} \end{aligned} \tag{2.6}$$

where L^k (for $k \in \mathbb{N}$) denotes k iterations of the map and L^0 is defined to be the identity map.

The orbit of a point z is just the sequence of points obtained by repeatedly iterating L for the point z. (For the time being, we ignore orbits of rational maps that will have singular points as we will deal with this at the end of this chapter). A special type of orbit is one that has a finite sequence of points.



(a) Filled Julia set of f_c with $c = 1 - \phi$ where $\phi = (1 + \sqrt{5})/2$ is the golden ratio from Wikimedia [72].



(b) (Filled) Julia set of f_c with $c = i$ from Wikimedia [45]. There is no interior so the filled Julia set is the same as the Julia set.

Figure 2.1

Definition 2.2.2. A point z is periodic with period k if $L^k z = z$ for the least positive integer k. We say z belongs to a k-cycle. Additionally, a point z is preperiodic if there are integers $s \geq 0, k \geq 1$ such that $L^{s+k} z = L^s z$, that is, some iterate of z is periodic.

The main objects of study for a map L are its orbits. For some maps, the behaviour of its orbits is difficult to solve in general, while for others it is well known and easily solved. For example, for $d = 1$ and a polynomial map f, we may consider the filled Julia set for f

$$J(f) = \{z \in \mathbb{C} \mid \text{ the orbit of } z \text{ is bounded}\} \tag{2.7}$$

whose boundary is the Julia set of f. A familiar complex dynamical system is given by quadratic polynomials, that is, $f : \mathbb{C} \to \mathbb{C}$ given by

$$f_c(z) = z^2 + c \tag{2.8}$$

for some $c \in \mathbb{C}$. Examples of the filled Julia set are given for $c = 1-\phi$ where $\phi = (1+\sqrt{5})/2$ and $c = i$ in figure 2.1. This is a special case of rational maps (which we will be considering in this thesis). We are interested in rational maps, although we do not consider them over $\mathbb{R}$ or $\mathbb{C}$ but instead over a discrete space, say $\mathbb{Q}$. An initial motivating problem is the how many periodic or preperiodic points are rational? We have an important result by Northcott [53]. Let $PrePer(f)$ denote the set of preperiodic points of the map f.

Theorem 2.2.3. *(Northcott 1950) Let $f : K^d \to K^d$ be a polynomial map of degree $n \geq 2$ defined over a number field K. Then*

$$PrePer(f) \cap K^d \text{ is finite.} \tag{2.9}$$

In particular, a rational function $f \in \mathbb{Q}[z]$ of degree $n \geq 2$ has only finitely many rational preperiodic (and periodic) points.

This is an interesting result as there are infinitely many complex periodic points, and in many cases even infinitely many real periodic points. Furthermore, Morton and Silverman [51] conjectured that for a polynomial map with fixed degree $n \geq 2$, the number of rational periodic points is bounded by a constant $C(d)$. For the map (2.8), it has been shown that for any c, there are no rational periodic points of period 4 by Morton [50] and period 5 by Flynn, Poonen, Schaefer [21]. Poonen [58] further conjectured that there are no rational points with period 6 or more.

Conjecture 2.2.4. *(Poonen 1998) If $N \geq 4$, then there is no quadratic polynomial $f(z) \in \mathbb{Q}[z]$ with a rational point of exact period N.*

This conjecture was verified by Hutz and Ingram [31] for (2.8) with rational c whose numerator or denominator (in absolute value) is less than or equal to 10^8. We now examine dynamical systems on a discrete space that is also finite.

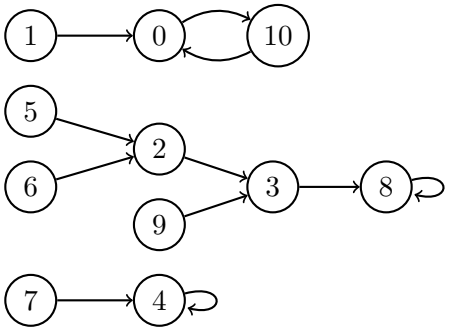
2.3 Finite dynamical systems

An interesting case to consider is when S is a finite set for which $L : S \to S$. Now every $z \in S$ must be periodic or preperiodic. In this case, we can fully describe the dynamics of L by simply computing the orbit of every point. For finite sets, a useful way to represent the dynamics is by using a directed (or functional) graph where each $z \in S$ is assigned a vertex and we have directed edges (z, Lz). Every vertex has exactly one edge leaving it, but may have zero, one or multiple edges entering it. A large class of these finite systems is for S taken to be a finite field $\mathbb{F}_p$ and L a polynomial over S. Recall that $\mathbb{F}_p = \{0, 1, 2, \ldots, p-1\}$ and all operations are done modulo p.

Example 2.3.1. Let $f : \mathbb{F}_{11} \to \mathbb{F}_{11}$ be defined by $f(x) = x^2 - 1$. Then we have the following table describing the function value of each point:

x	0	1	2	3	4	5	6	7	8	9	10
$f(x)$	10	0	3	8	4	2	2	4	8	3	0

The directed graph corresponding to the map f is given by



Here we have 3 disjoint components, one with a 2-cycle and two with fixed points.

Notice that the directed graph consists of disjoint components, each with one cycle. In general, we are interested in questions related to the structures seen in the directed graph, for example,

- How many cycles are there?
- How long are the cycles?
- What is the distribution of the lengths of the cycles?

We may also ask similar questions about the preperiodic points in each disjoint component. Of course, given a particular finite field $\mathbb{F}_q$ and polynomial f, we can explicitly compute these statistics by direct computation but the goal is in understanding the mathematical factors behind what we see which will enable us to comment about the dynamics for a general finite field and polynomial.

The study of discrete dynamics over finite fields has for the most part been a recent phenomena. The simplest dynamical systems (over finite fields) are linear. Elspas (1959) [19] studied four dimensional linear systems modulo 2 for which he deduced necessary conditions for the cycle structure by using the elementary divisors of the associated matrix. Percival and Vivaldi (1987) [55] studied linear systems on rational points of the 2-torus (reducing to finite rational lattices) using ideal theory and showed that all orbits are periodic with the same cycle length. Vivaldi (1992) [77] studied the geometry of the orbits of linear maps in two dimensions. For nonlinear maps over finite fields, the dynamics can be much more exotic and its study is in general quite complicated. One of the

applications of these dynamical systems is for pseudorandom number generation. A well known example using this property was given by Pollard (1975) [57] in his famous paper on integer factorisation, which was hinged on the behaviour of the quadratic polynomial map in $\mathbb{F}_p$ given by

$$f(x) = x^2 - 1. \tag{2.10}$$

He suggested that quadratic polynomials modulo large primes behave like random mappings on $\mathbb{F}_p$ and used this fact to estimate the expected cycle lengths and pretail lengths allowing him to give probabilistic arguments for the number of steps required before finding a prime factor. Martins and Panario (2016) [47] provided heuristic arguments that support this idea for quadratic polynomials and also for higher degrees by looking at the rho length of the nodes. Furthermore, Benedetto et al. [6] also considered the normalised cycle lengths of degree 2 polynomial maps over $\mathbb{F}_p^d$ (for $d = 1, 2, 3$) and showed that it follows random mapping behaviour modulo p. We will use these ideas in chapter 3 and 4 to construct a model for the number of cycles in polynomial automorphisms and birational maps. The difficulty in studying even quadratic polynomials over finite fields is evident as even now, some 40 years later, their behaviour is still not fully understood in general except for the maps $x' = x^2 \pmod{p}$ which was studied by Rogers (1996) [65] and $x' = x^2 - 2 \pmod{p}$ studied by Gilbert et al. (2001) [24] and Vasiga and Shallit (2004) [76].

2.4 Expected statistics of polynomial maps

The complexity of these systems has led some to consider the "average statistics" for particular classes of maps. Chou and Shparlinski [14] studied the average values of various statistics for repeated exponentiation $x' = x^e \pmod{p}$ for some integer $e \geq 2$, which was extended by Sha [69] modulo prime powers. The idea of average statistics is an important idea in this thesis. We want to be able to say something about the behaviour of a general dynamical system described by some polynomial (or rational) map by looking at expected statistics as, for example, even quadratic maps like (2.10) are not fully understood. Then, depending on the distribution of the maps, we may be able to say something about the expected statistics of a randomly chosen map from a given class of maps (e.g. degree 2 polynomials). We may wonder how random maps compare to polynomial maps (of a given degree). Random maps are more general than polynomial maps and in some aspects are easier to handle since they are less restrictive. Flajolet and Odlyzko [20] used generating

functions to find the expected statistics for various properties of random maps of n points such as the number of components, cyclic points, terminal points and image points in the directed graph representation. Their asymptotic forms as $n \to \infty$ are

$\#Components$	$\frac{1}{2}\log n$
$\#Cyclic\ points$	$\sqrt{\pi n/2}$
$\#Terminal\ points$	$e^{-1}n$
$\#Image\ points$	$(1-e^{-1})n$

where a point is cyclic if it belongs to a periodic cycle, a point is terminal if it has no preimage and is an image point otherwise. They also found the expected statistics when seen from a random point in a random mapping for the tail length, cycle length, rho length, tree size, component size and predecessor size. These results may be used to model quadratic (or higher degree) polynomial maps. However, one may argue that random mappings do not accurately represent the behaviour of polynomial maps as they do not take into account that any point in a polynomial map with degree d has a preimage set of size at most d. Thus, understanding the behaviour of polynomial maps is important. Arney and Bender [2] considered random mapping statistics with constraints on the number of origins and indegrees of points. Using this model may be more accurate but it still may not take into account all the intricacies of polynomial maps. For example, in quadratic maps defined by degree 2 polynomials, it is easy to show that the functional graph has one node with indegree 1, $(p-1)/2$ with indegree 2 and the remaining $(p-1)/2$ with indegree 0 (for example see the directed graph of example 2.3.1.

We may ask what the expected statistics are for degree d polynomial maps and how do they compare with random maps. For example, Kruskal [36] showed that the expected number of components for a random map on n points is given by

$$\mathcal{K}(n) = \frac{1}{2}\log n + \left(\frac{\log 2 + \psi}{2}\right) + o(1) \tag{2.11}$$

where $\psi = 0.5772156649...$ is the Euler-Mascheroni constant. For polynomial maps of degree d over $\mathbb{F}_q$, Flynn and Garton [22] obtained upper and lower bounds on the average number of components and periodic points. Furthermore, Bellah et al. [5] provided a

probabilistic heuristic to count the number of components for the same polynomial maps of degree d and found that this was equal to

$$\mathcal{K}(q) + O(1) \tag{2.12}$$

under some mild conditions. This gives some evidence that the expected statistics of polynomial maps may not be too dissimilar to the expected statistics of random maps. Konyagin et al. [35] also noted from their numerical tests that the average values of the number of periodic points and the size of the largest connected components for polynomial maps behave like random maps.

Another problem of interest is how many different or non-isomorphic functional graphs (that is, different dynamical systems) we obtain when considering all degree d polynomial maps. Bach and Bridy [3] considered the problem of finding $D_q(d)$, the number of non-isomorphic functional graphs of affine maps over the d dimensional space $\mathbb{F}_q^d$ obtaining the bound:

Theorem 2.4.1. *(Bach and Bridy 2013) For fixed q and $d \to \infty$*

$$\sqrt{d} \ll \log D_q(d) \ll \frac{d}{\log \log d}. \tag{2.13}$$

Further, Konyagin et al. [35] considered degree m polynomials over $\mathbb{F}_q$ and obtained bounds on the number of non-isomorphic functional graphs. In particular, their results showed that for quadratic maps this number $N_2(p)$ is

$$p^{1/4+o(1)} \leq N_2(p) \leq p \tag{2.14}$$

for $q = p$ an odd prime. Interestingly, from their experiments they found that $N_2(p) = p$ except for $p = 2, 17$ but noted that it may be difficult to prove as "there is no intrinsic reason for this to be true". This shows the difficulty of providing exact results for dynamical systems as even the quadratic case is extremely complex. These numbers were further considered by Ostafe and Sha [54] for polynomials of special forms. Furthermore, Bridy and Garton [9] considered the family of maps $x^k + m$ over $\mathbb{F}_p$ and showed that for any positive integers k, M greater than 1, there are infinitely many sets of integers of size M such that the family of maps are dynamically non-isomorphic as $p \to \infty$. For more

references of univariate dynamics over finite fields see this recent survey on iterations of mappings over finite fields [46].

2.5 Permutation mappings

A special type of mapping is one that is bijective on a finite set. These are called *permutation mappings*, and more specifically if the mapping is a polynomial, then we call them *permutation polynomials*. It is natural to consider polynomial mappings since every permutation g over a finite field $\mathbb{F}_q$ can be expressed as a polynomial by Lagrange interpolation,

$$P_g(x) = \sum_{a \in \mathbb{F}_q} g(a)(1 - (x - a)^{q-1}). \tag{2.15}$$

Dickson [18] in 1897 first introduced a class of permutation polynomials now known as Dickson polynomials. Lidl and Mullen [41] in 1988 provided the major known classes of permutation polynomials and presented a list of nine open questions related to them. Since then, there has been increased attention and research in this area, for example, in determining which polynomials f are permutation polynomials and efficient tests for whether a given f is one. This led to work by Gathen [23] providing a probabilistic test using $O(d \log q)$ operations while Shparlinski [71] provided a deterministic method in time $O(dq)^{6/7+\epsilon}$. It is difficult to find or count all the permutation polynomials in a finite field. The importance of the Dickson polynomials is due to a claim known as Schur's conjecture. Schur proved that every integral polynomial (a polynomial with integer coefficients) of prime degree which is a permutation polynomials for infinitely many p, is a composition of Dickson polynomials and linear polynomials. The conjecture was whether this statement is also true for integral polynomials of general degree, which was proved in 1995 by Turnwald [75].

For specific classes of permutation polynomials, their cycle structure is known. A monomial $f_k(x) = x^k$ is a permutation polynomial of $\mathbb{F}_q$ if and only if $\gcd(k, q-1) = 1$. Ahmad (1969) [1] studied the cycle lengths of permutation monomials and found criteria for specific cycle lengths and the number of them using elementary number theory. Rubio and Corrada (2004) [67] provided conditions for which these maps have all cycles of the same

length (ignoring fixed points). The Dickson polynomial polynomials of the first kind are given by

$$D_n(x,\alpha) = \sum_{i=0}^{\lfloor n/2 \rfloor} \frac{n}{n-i}\binom{n-i}{i}(-\alpha)^i x^{n-2i}. \tag{2.16}$$

This is a permutation polynomial if and only if $\gcd(i, q^2-1) = 1$. Rubio et. al. (2008) [68] showed conditions for which the cycle lengths of the Dickson polynomials are the same for $\alpha = -1, 0, 1$. Furthermore, the cycle lengths and the structure of the functional graphs of Rédei functions were classified in [66] and [59] respectively. The Dickson polynomials can be seen as a generalisation of these as monomials correspond to the case $\alpha = 0$.

Through this brief review of some results in the area of maps over finite fields, we learn some useful things. Even in one dimension, the dynamics of polynomial maps can be very complicated, for which there are still many open problems. When we increase the dimensions, this increases the complexity further. However, there are two ways which we can make progress. Firstly, we can look at specific maps, or specific families of maps which may have certain properties for which we may be able to obtain various results. Alternatively, if we are interested in more general, larger classes of maps, instead of solving its dynamics exactly, we can look at its expected behaviour.

2.6 Polynomial automorphisms and birational maps in higher dimensions

In this thesis, we will be working with the field K in (2.1) being the finite field $\mathbb{F}_p$. Furthermore, we will study polynomial maps L over $\mathbb{F}_p^d$ that have an inverse that is also a polynomial map which we denote by L^{-1}. Necessarily, L and L^{-1} must be one-to-one and we have

$$LL^{-1}z = z, \qquad L^{-1}Lz = z \tag{2.17}$$

for all $z \in \mathbb{F}_p^d$. Such maps L (and L^{-1}) are called *polynomial automorphisms*. Studying these higher dimensional maps greatly increases the complexity of the system (compared to $d = 1$) as these mappings are now a system of equations with multiple variables. We are interested in how specific algebraic properties of a mapping manifest themselves (if they do) in the finite space. Some results and ideas from permutation polynomials can be extended to higher dimensions. For example, Maubach (2001) [48] showed that higher dimensional polynomial automorphisms over $\mathbb{F}_q^d$ give all possible bijections (or permutations) for $q = 2$ or $q = p^r$ where $p > 2$. A similar result was given by Cantat (2009)

[11] showing that every permutation on $\mathbb{F}_q^d$ is induced by a birational transformation. This means that we can obtain all possible permutations by considering only polynomial maps. The increase in complexity of these systems raises the question of how we may study general nonlinear maps of this type. The results above by Maubach and Cantat also support the possibility that the observed statistics of a (random) permutation polynomial may be similar to the average statistics of a random permutation. We examine this idea by first finding the expected statistics for random permutations and comparing them to permutation mappings in higher dimensions in chapter 3.

We also consider rational mappings L over $\mathbb{F}_p^d$ that also have a rational inverse L^{-1} where defined. That is, we have (recalling (2.4))

$$LL^{-1}z = z, \qquad z \notin \mathrm{Sing}(L^{-1}) \text{ and } L^{-1}z \notin \mathrm{Sing}(L), \tag{2.18}$$

$$L^{-1}Lz = z, \qquad z \notin \mathrm{Sing}(L) \text{ and } Lz \notin \mathrm{Sing}(L^{-1}). \tag{2.19}$$

Here L, L^{-1} must be one-to-one (on the restricted spaces where they are defined). These will be called *birational maps*. Note that the orbit of a point terminates in the affine space when it hits a singular point of L. To account for orbits with singular points, we redefine the orbit of a point for birational maps.

Definition 2.6.1. Suppose L is a birational map with inverse L^{-1}. The forward orbit of a point z is given by

$$\sigma_F(z) = \{L^k z, k \in \mathbb{N} \mid L^j z \notin \mathrm{Sing}(L), 0 \le j \le k\}, \tag{2.20}$$

and the backward orbit of a point z is given by

$$\sigma_B(z) = \{L^{-k} z, k \in \mathbb{N} \mid L^{-j} z \notin \mathrm{Sing}(L^{-1}), 0 \le j \le k\}, \tag{2.21}$$

and the orbit is given by

$$\sigma(z) = \sigma_F(z) \cup \sigma_B(z). \tag{2.22}$$

The forward orbit is the largest sequence of points obtained by iterating L until hitting a singular point or returning to itself and similarly the backward orbit is the same but for L^{-1}. We call any orbit with a point in $\mathrm{Sing}(L) \cup \mathrm{Sing}(L^{-1})$ to be a *singular orbit*. For

periodic orbits, definition 2.6.1 is identical to definition 2.2.1. The orbit decomposition of L consists of a disjoint union of periodic and singular orbits. The number and distribution of these orbits is of interest and this is what we investigate in chapter 4 which can be seen as an extension of the ideas in chapter 3. We will propose a model for the expected number of these statistics and show that typically, a birational mapping has similar statistics.

Chapter 3

Random permutations and polynomial automorphisms over finite fields

A d-dimensional polynomial automorphism over the finite space $\mathbb{F}_p^d$ is a permutation of the space. It provides a realisation of one of the elements of the symmetric group S_{p^d}. Thus, the orbits decompose into a finite number of periodic orbits (or cycles). In this chapter, we review some statistical properties and expectations for permutations on n points. In particular, we are interested in the number of cycles, and the distribution of their lengths. In other words, if we randomly choose an element from the symmetric group S_n, what do we expect to see? We compare these expected values with the observed statistics for deterministic polynomial automorphisms and show that this is a good model for the number of cycles. Practically speaking, this means that we expect a randomly chosen polynomial automorphism (with no structural constraints) to behave like a random permutation.

3.1 Random permutations

Let σ be a permutation on n points, e.g. $(1, 2, 3, \ldots, n)$, of which there are $n!$ permutations. Each permutation has a corresponding cycle decomposition consisting of a disjoint union of cycles of various lengths. Let C_k be the number of k-cycles (cycles of length k) of σ. We have the constraint that

$$\sum_{k=1}^{n} kC_k = n. \tag{3.1}$$

Let $C := \sum_{k=1}^{n} C_k$ be the number of cycles. This has minimum value 1 when the permutation has one cycle of length n, and maximum value n when the permutation consists of

n fixed points. The following results on random permutations can be found in many texts for example see [26, 49, 70]. Let σ be a randomly chosen among the $n!$ permutations.

Theorem 3.1.1. *The expected number of k-cycles (in a permutation of n points) is $E_n(C_k) = 1/k$ for $1 \leq k \leq n$.*

Proof. We construct all possible k-cycles and divide by the size of the probability space $\#S_n = n!$. To construct a k-cycle from n points, we first choose the k points from n in $\binom{n}{k}$ ways and then arrange these points into a cycle in $\frac{k!}{k}$ ways. Then we assign the rest of the $n-k$ points which can be done in $(n-k)!$ ways. Multiplying these together and dividing by $n!$ yields

$$\frac{\binom{n}{k}k!(n-k)!}{n!k} = \frac{1}{k}. \tag{3.2}$$

□

Corollary 3.1.2. *The expected number of points belonging to k-cycles is 1 point.*

This follows directly from theorem 3.1.1 since $kE_n(C_k) = 1$ for all $1 \leq k \leq n$. This follows the discrete uniform distribution, that is, for a random permutation, the probability that a chosen point belongs to a cycle of any length is equiprobable. The cumulative distribution function is a step-function with n steps of height $\frac{1}{n}$. If we scale the cumulative distribution by n, in the limit, we get $\mathcal{D}_n(x) = x,\ 0 \leq x \leq 1$.

Theorem 3.1.3. *The expected number of cycles $E_n(C)$ is*

$$H_n = \sum_{k=1}^{n} \frac{1}{k} = 1 + \frac{1}{2} + \frac{1}{3} + \ldots + \frac{1}{n} = \log n + \psi + O\left(\frac{1}{n}\right), \tag{3.3}$$

where $\psi \approx 0.5772156649$ is the Euler-Mascheroni constant.

Proof. This is a well known result and follows directly from theorem 3.1.1 since

$$E_n(C) = E_n(\sum_{k=1}^{n} C_k) = \sum_{k=1}^{n} E_n(C_k) = \sum_{k=1}^{n} \frac{1}{k} = H_n. \tag{3.4}$$

□

Theorem 3.1.4. *The variance of the number of cycles is*

$$H_n - \sum_{i=1}^{n} \frac{1}{i^2}. \tag{3.5}$$

Proof. The number of permutations on n points with m cycles is by definition the unsigned Stirling number of the first kind $\left[{n \atop k}\right]$ which satisfies the recurrence

$$\left[{n \atop m}\right] = (n-1)\left[{n-1 \atop m}\right] + \left[{n-1 \atop m-1}\right] \tag{3.6}$$

for $k > 0$ and initial conditions $\left[{0 \atop 0}\right] = 1$, $\left[{n \atop 0}\right] = 0$. This can be understood combinatorially, since there are two ways to form a permutation with m cycles from n objects from a permutation of $n-1$ objects. The nth object can be a fixed point which increases the cycle count by 1, so this accounts for the $\left[{n-1 \atop m-1}\right]$ term. Also, this nth object could be added to one of the cycles. In this case, the cycle count stays the same, and there are $n-1$ ways to add this point into a permutation of $n-1$ with m cycles (1 way after each object). Let $P_n(m)$ be the probability of choosing at random a permutation with m cycles. Then,

$$P_n(m) = \frac{\left[{n \atop m}\right]}{n!}, \tag{3.7}$$

and by applying the recurrence we have,

$$P_n(m) = \frac{n-1}{n} P_{n-1}(m) + \frac{1}{n} P_{n-1}(m-1). \tag{3.8}$$

To find the variance we use the well known identity $Var_n(C) = E_n(C^2) - [E_n(C)]^2$. Then using (3.8) we have,

$$E_n(C^2) = \sum_{m=1}^{n} m^2 P_n(m) = E_{n-1}(C^2) + \frac{2}{n} E_{n-1}(C) + \frac{1}{n}, \tag{3.9}$$

where $E_n(C) = H_n$ and hence

$$E_n(C^2) = H_n + 2\sum_{i=1}^{n-1} \frac{H_i}{i+1}. \tag{3.10}$$

Thus,

$$Var_n(C) = H_n - \sum_{i=1}^{n} \frac{1}{i^2}, \tag{3.11}$$

since $\sum_{i=1}^{n-1} \frac{H_i}{i+1} = \frac{1}{2}H_n^2 - \frac{1}{2}\sum_{i=1}^{n} \frac{1}{i^2}$. □

Note that as $n \to \infty$, the sum $\sum_{i=1}^{n} \frac{1}{i^2} = \frac{\pi^2}{6}$ and so for $n \geq 1$

$$1 \leq \sum_{i=1}^{n} \frac{1}{i^2} < \frac{\pi^2}{6} < 1.65. \tag{3.12}$$

Knowing the distribution of the number of cycles of a random permutation provides us with more information on what we expect to see for repeated experiments, and also how far we expect the observed values to be from the mean. The following asymptotic distribution results were derived by Goncharov in 1942.

Theorem 3.1.5. *[26] For a random permutation on n points, the distribution of the number of k-cycles C_k converges in distribution to the Poisson distribution with parameter $\frac{1}{k}$. That is,*

$$\lim_{n\to\infty} P_n\{C_k = a\} = e^{-1/k}\frac{(1/k)^a}{a!}, \qquad a = 0, 1, \ldots, \tag{3.13}$$

Theorem 3.1.6. *[26] The number of cycles C for a random permutation on n points converges in distribution to the Normal distribution with mean H_n and variance H_n. That is,*

$$\lim_{n\to\infty} P\left(\frac{C - \log n}{\sqrt{\log n}} \leq x\right) = \phi(x) = \frac{1}{\sqrt{2\pi}}\int_{-\infty}^{x} e^{-u^2/2}du. \tag{3.14}$$

In figure 3.1 we plot the results for the number of cycles for a sample of 5000 randomly chosen permutations on $n = 10000$ points. The variance of the distribution provides how much we expect samples to vary from the mean. We see its closeness with the (discretised) normal distribution.

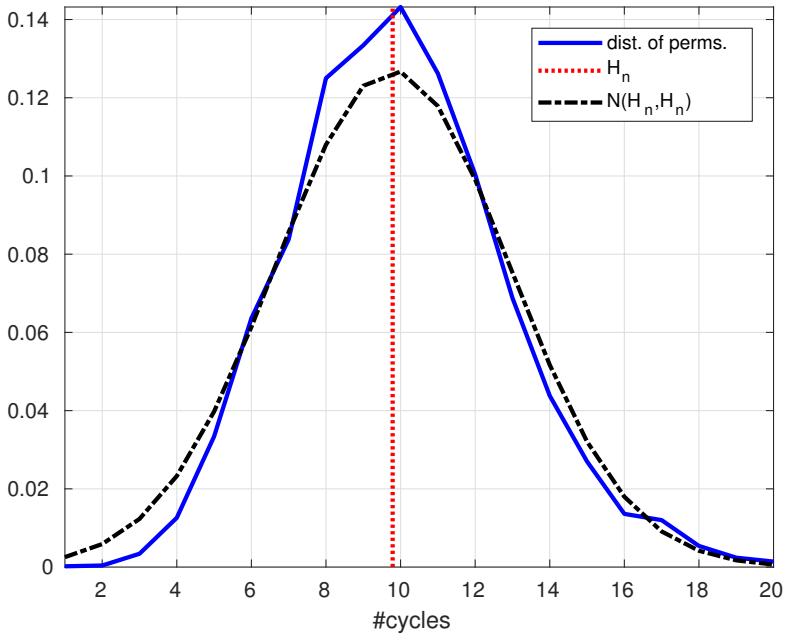


Figure 3.1: Distribution of the number of cycles for 5000 permutations of $n = 10000$ points chosen randomly, compared to the discretised normal distribution with mean and variance H_n.

3.2 Random permutations vs polynomial automorphisms

In this section, we compare the statistics of random permutations with the observed statistics for polynomial automorphisms over finite fields. Since the latter induce permutations of the space, and the action modulo p seems to "randomise" the iterations of the mapping, we may expect to see similar statistics for the cycles of polynomial automorphisms as seen in random permutations.

The concept of a mapping over a finite field acting "randomly" need not be an unfamiliar idea or concept. Bober [8] studied the behaviour of the inverse mapping $B : x \to x^{-1}$ over a finite field as a permutation of the integers from 1 to $p-1$. The mapping B is bijective on $\mathbb{F}_p - \{0\}$, and so $1^{-1}, 2^{-1}, \ldots, (p-1)^{-1}$, each taken modulo p defines the image of a permutation of $1, 2, \ldots, p-1$. This mapping is an involution with 2 fixed points 1 and $-1 = p-1 \pmod{p}$. Bober examined the "randomness" of this map by comparing the distribution of the length of the longest increasing subsequence to that of a random fixed-point-free signed involution, and showed asymptotically, they were the same. Notice that Bober did not compare to the statistics to a random permutation, but restricted it to a more specific class of maps, random fixed point free signed involutions. Also, recall the examples of Pollard, Martins and Panario, and Bendetto et al. mentioned in chapter 2 which used and heuristically justified the use of random mapping models for

polynomial maps. Using random mapping models for polynomial or rational maps will be a common theme in this thesis when examining cycle statistics. If we know a map has a specific property or structure, it is reasonable to compare it with the expected statistics of an object with the same property or structure. However, one shortcoming or difficulty of this is that it may be difficult to know some properties of a map a priori.

3.2.1 Dissipative Hénon map

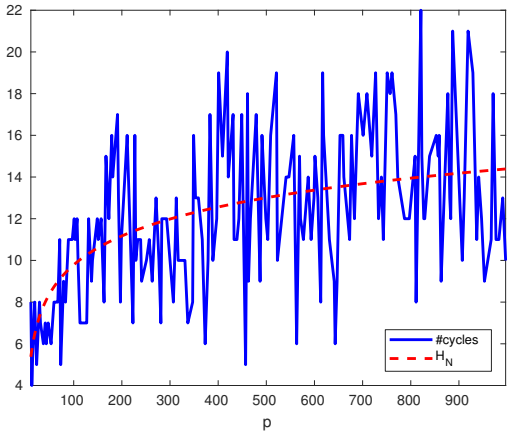
Consider the two parameter (non-reversible) dissipative Hénon map over $\mathbb{F}_p^2$ given by

$$H\acute{e}non_{dis} : \; x' = y, \qquad y' = -\delta x + y^2 + \epsilon \tag{3.15}$$

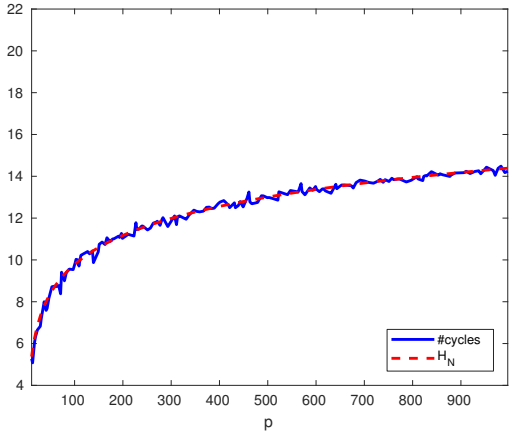
for $\epsilon \in \mathbb{F}_p$ and $\delta \in \mathbb{F}_p \setminus \{0, 1\}$. Over $\mathbb{R}^2$ the map (3.15) is famous for possessing a chaotic fractal attracting set [29]. We disallow $\delta = 0$ since the mapping will be essentially one dimensional, and $\delta = 1$ since then the mapping will be "reversible". (The definition of reversible and this latter case is considered in chapter 5.) Over $\mathbb{F}_p^2$, (3.15) is a permutation with inverse given by

$$H\acute{e}non_{dis}^{-1} : \; x' = \frac{1}{\delta}(-y + x^2 + \epsilon), \qquad y' = x. \tag{3.16}$$

We take this map to be a representative polynomial automorphism. For each prime, we consider the cycle decomposition focusing on the number of cycles. Figure 3.2 shows the number of cycles for the dissipative Hénon map over primes compared to the Harmonic number H_{p^2} of (3.3). On the left, for each prime we have $\delta = 2$ and $\epsilon = 1$ while on the right we average over $\delta = 2, \ldots, p-1$ with $\epsilon = 1$. Recall from theorem 3.1.3 that a random permutation of p^2 points is expected to have this number of cycles. Figure 3.2 shows preliminary evidence that the expected cycle statistics of a random permutation is a good model for a non-reversible polynomial automorphism. From observations, maps with cubic, quartic or higher degree polynomials also exhibit similar behaviour. We may also compare the number of points belonging to k-cycles to the expected number for a random permutation in corollary 3.1.2. To do this, we average over ϵ for $\epsilon = 0, \ldots, p-1$ as shown in figure 3.3. The expected number for a random permutation is shown in red. Note here that the possible range of values for the number of points in k-cycles is $[0, p^2]$. Roberts and Vivaldi [63] conjectured that an averaged scaled period distribution of planar polynomial maps over $\mathbb{F}_p^2$ has a universal distribution as $p \to \infty$. They also showed experimentally



(a) The number of cycles for the dissipative Hénon map with $\epsilon = 1, \delta = 2$ for primes $p = 11 \ldots 997$ compared with the probabilistic model using random permutations.



(b) The number of cycles for the dissipative Hénon map with $\epsilon = 1$ averaged over the $p - 2$ values $\delta = 2, \ldots, p - 1$ for primes $p = 11 \ldots 997$ compared with the probabilistic model using random permutations.

Figure 3.2

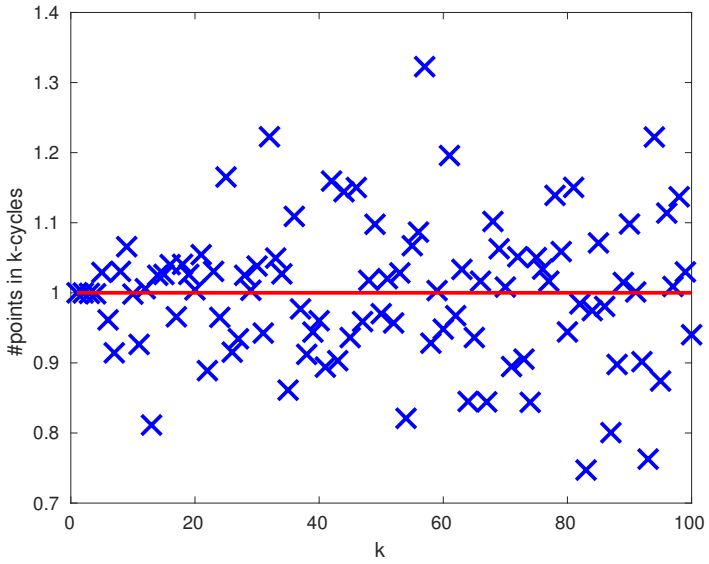
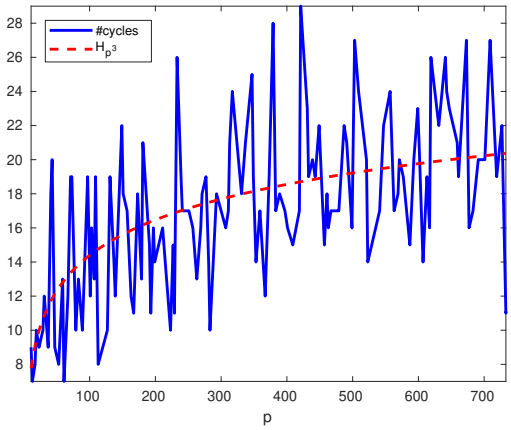


Figure 3.3: The number of points belonging to cycles of length k for the dissipative Hénon map with $\delta = 2$ for $p = 4999$ averaged over $\epsilon = 0, 1, \ldots, p - 1$. Note the expected number of points in k-cycles for a random permutation is 1 (independent of k).

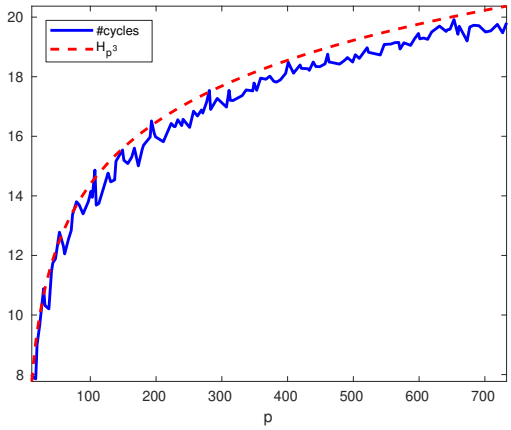
that the expected maximum cycle length and the expected number of cycles of such a map were well modelled by random permutation statistics.

3.2.2 Dissipative Hénon map in 3D

Consider the following three dimensional polynomial automorphism in $\mathbb{F}_p^3$ where the first two coordinates are the same as the 2D Hénon map (3.15) (with ϵ replaced with z) and



(a) Number of cycles for the map in (3.17) with $\delta = 2$ for primes $p = 11, \ldots, 733$. This is compared with the expected number using the random permutation model from equation (3.3).



(b) Number of cycles for the map in (3.17) averaged over $\delta = 2, \ldots, p-2$ for primes $p = 11, \ldots, 733$ compared with the probabilistic model using random permutations.

Figure 3.4

we add a third coordinate,

$$H\acute{e}non3D_{dis} : x' = y, \qquad y' = -\delta x + y^2 + z, \qquad z' = x + y + z + 1 \tag{3.17}$$

for $\delta \neq 0, 1, p-1$. We expect this to behave like a random permutation on p^3 points and thus the number of cycles will be approximately $H_{p^3} \approx \log(p^3)$. We plot this in figure 3.4 for $\delta = 2$ on the left and averaged over δ on the right. Again, even in three dimensions, we see a good fit between the expected cycles in a random permutation and the polynomial automorphism. (Recall that the number of cycles can range between 1 and p^3.) We see that the dynamics of the polynomial automorphisms seems to be dependent only on the number of points, and independent of dimension. For example for primes p_1, p_2 such that $p_2 \approx p_1^{2/3}$ we expect a two dimensional polynomial automorphism over $\mathbb{F}_{p_1}^2$ to have similar cycle statistics to a three dimensional map over $\mathbb{F}_{p_2}^3$.

3.3 Concluding Remarks

In this chapter, we reviewed some well known properties and statistics of random permutations, in particular with regard to the number of (k-cycles and) cycles. The main result is that the expected number of cycles of a permutation on n points is given by the nth Harmonic number $H_n \approx \log n$. This result is surprising in a way as it is quite small when we consider that a permutation can have up to n cycles. We also saw that this number

was asymptotically normally distributed emphasising the "niceness" of this statistic. We then compared this with the number of cycles in two polynomial automorphisms over the finite field in two and three dimensions. There is no inherent reason why they should give similar statistics but intuitively we can say that generally, (non-linear) polynomial automorphisms act "randomly" in the finite space. The discreteness and action modulo p mixes the points so it seems like the map is like a random permutation even though it is completely deterministic. Here we are not saying that polynomial automorphisms and random permutations are equivalent but there are similarities which can be exploited. We will use this idea when we examine the statistics of birational maps in chapter 4 and compare them to a model with similar restrictions and properties of the initial map, and it will be used in chapter 8 when considering the statistics of the composition of two involutions. The examples in this chapter serve as a taster for what is to come in this thesis. For different maps, we will need to employ different suitable combinatorial models as a comparison.

Chapter 4

Random s-permutations and birational maps over finite fields

We consider rational mappings L over the finite space $\mathbb{F}_p^d$ that also have a rational inverse L^{-1} where defined. So each coordinate is defined by a rational function, that is, we can write L (and similarly L^{-1}) as

$$x_1' = \frac{f_1(x_1, x_2, \ldots, x_d)}{h_1(x_1, x_2, \ldots, x_d)} \tag{4.1}$$

$$x_2' = \frac{f_2(x_1, x_2, \ldots, x_d)}{h_2(x_1, x_2, \ldots, x_d)} \tag{4.2}$$

$$\vdots = \vdots \tag{4.3}$$

$$x_d' = \frac{f_d(x_1, x_2, \ldots, x_d)}{h_d(x_1, x_2, \ldots, x_d)} \tag{4.4}$$

where f_i, h_i are polynomials in $x_1, x_2, \ldots, x_d$. This map is not defined for the set $\mathrm{Sing}(L) = \{(x_1, x_2, \ldots, x_d) \mid h_i(x_1, x_2, \ldots, x_d) = 0, \text{ for some } i = 1, \ldots, d\}$. Then L is a birational mapping over $\mathbb{F}_p^d$ and we have

$$LL^{-1}z = z, \qquad z \notin \mathrm{Sing}(L^{-1}) \text{ and } L^{-1}z \notin \mathrm{Sing}(L) \tag{4.5}$$

$$L^{-1}Lz = z, \qquad z \notin \mathrm{Sing}(L) \text{ and } Lz \notin \mathrm{Sing}(L^{-1}). \tag{4.6}$$

We call any orbit (see definition 2.6.1) with a point in $\mathrm{Sing}(L)$ to be a *singular orbit*. This point will be the "last point" in the forward orbit of L. Necessarily, due to L being a birational map, this orbit will also have a point in $\mathrm{Sing}(L^{-1})$ which will be the "last point" in the forward orbit of L^{-1}. The orbit decomposition of L consists of the partition of space into periodic and singular orbits. The number and distribution of these orbits is of interest and this is what we investigate in this chapter. We present a probabilistic model which mimics a birational map. We count the expected statistics of this model and show

that typically, a birational mapping has similar statistics by comparing it to "randomly" chosen birational maps. This idea supposes that the details of the mapping aren't that important, and the statistics are mainly constrained by the cardinality of singular sets and phase space size, and that maps with the same numbers of these values appear to behave similarly, and the same as our model.

4.1 Setting out the model

We now describe a new object which simulates a birational map. All of the following definitions have direct correspondences with birational maps.

Let N, s be integers with $0 \leq s < N$. Let $[N] = \{1, 2, \ldots, N\}$, and S be an s-subset of $[N]$ (a subset of $[N]$ containing exactly s points). Let $f : [N] - S \to [N]$ be a one-to-one function and let $W(N, s)$ be the set of all such functions f. We will call f an *s-permutation* (on N).

Definition 4.1.1. S is called the *singular set* and a point z is called a *singular point* if $z \in S$.

Definition 4.1.2. A point z is called an *origin point* if there does not exist $y \in [N] - S$ such that $f(y) = z$.

Origin points are the points with no pre-image, that is, we cannot get to them by applying f to any point in its domain. Since f is a one-to-one function, the number of origin points is s. We denote the set of origin points as $\bar{S}$. We call $\bar{S}$ the *origin set*.

Definition 4.1.3. The forward orbit of a point z is the set of points $\sigma_F(z) = \{f^j(z) \mid f^{j-1}(z) \notin S, j \in \mathbb{Z}^+\} \cup \{z\}$.

This is the set of points obtained by repeatedly iterating f (until we return or reach a singular point). Suppose that f has origin set $\bar{S}$. Note that we can consider the equivalent map $\bar{f} : [N] - S \to [N] - \bar{S}$ where $f(a) = b \implies \bar{f}(a) = b$. This is well defined. We now mean $\bar{f}$ when we use f. Then we define the inverse of $\bar{f}$ which we also call the inverse of f.

Definition 4.1.4. The inverse function $f^{-1} : [N] - \bar{S} \to [N] - S$ is defined as follows: $f^{-1}(z) = y \iff f(y) = z$.

The inverse function is well defined and one-to-one since f is one-to-one.

Definition 4.1.5. The backward orbit of a point z is the set of points $\sigma_B(z) = \{f^{-j}(z) \mid f^{j-1}(z) \notin \bar{S}, j \in \mathbb{Z}^+\} \cup \{z\}$.

Definition 4.1.6. The orbit of a point z is the union of its backward and forward orbits, $\sigma(z) = \sigma_F(z) \cup \sigma_B(z)$.

Definition 4.1.7. A point z is a *periodic point* if there exists a positive integer k such that $f^k(z) = z$ and the smallest such k is its period.

If a point is periodic, then its forward orbit is the same as its backward orbit. The following is now clear:

Lemma 4.1.8. *Suppose that z is not a periodic point. Then there exists a non-negative integer k such that $f^k(z) \in S$, and a non-negative integer l such that $f^{-l}(z) \in \bar{S}$. We say that the orbit of z is a singular orbit of length $k + l + 1$.*

This is the natural definition of the length of the orbit, being its cardinality.

Definition 4.1.9. The *orbit decomposition* of an s-permutation is the partition of $[N]$ into disjoint orbits. Following the cycle notation of permutations, we can also have a similar cycle notation for s-permutations. We enclose periodic orbits (as before) with round brackets and singular orbits with square brackets. With this notation, for singular orbits the leftmost element in a square bracket is an origin point and the rightmost element is a singular point. We call this *orbit* notation.

Example 4.1.10. Let $N = 7$ and $s = 2$. Then our phase space is the set $[N] = \{1, 2, 3, 4, 5, 6, 7\}$ consisting of 7 points. Let $S = \{4, 7\}$ and so $[N] - S = \{1, 2, 3, 5, 6\}$. Suppose we have f with

$$f(1) = 2, f(2) = 6, f(3) = 7, f(5) = 4, f(6) = 1.$$

The set $\bar{S}$ of origin points is given by $\{3, 5\}$. The orbit decomposition of f has 3 disjoint orbits, a periodic orbit of length 3 and two singular orbits each of length 2, which can be written in our above-mentioned orbit notation as (126)[37][54].

4.1.1 Connection to random permutations

Construction 4.1.11. We can construct an s-permutation from a permutation $\hat{f}$ in the following way. Let $\hat{f}$ be a bijection from $[N]$ to itself. Choose an s-subset of $[N]$ and consider the mapping $f : [N] - s \to [N]$ where $f(n) = \hat{f}(n)$ for $n \in [N] - s$. Then f is an s-permutation. If $s = 0$, then $f = \hat{f}$ which is a permutation.

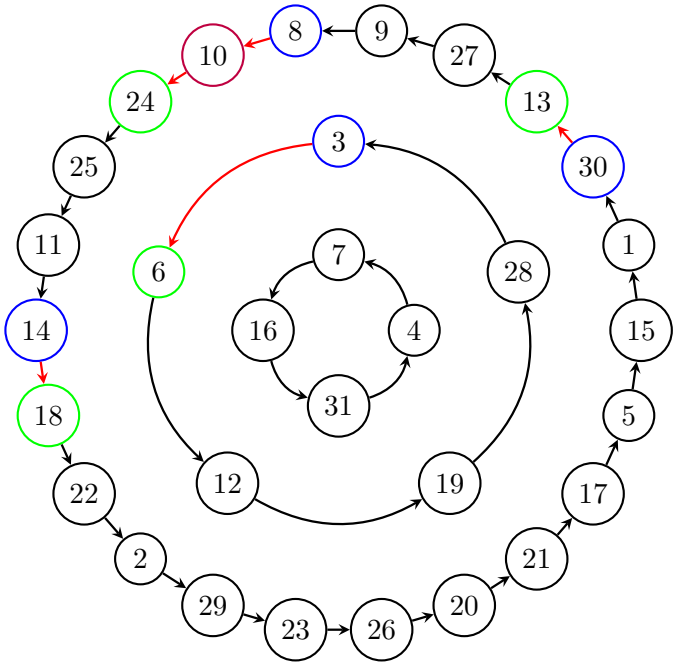


Figure 4.1: Orbit decomposition of a permutation on 31 points and a corresponding s-permutation obtained from this by choosing the 5-subset $\{3, 8, 10, 14, 30\}$. The edges removed are coloured in red. Singular points are coloured in blue, origin points in green. We colour points that are both singular and origin points in purple.

For example, consider the permutation with $N = 31$ given in cycle notation by

$$(13\ 27\ 9\ 8\ 10\ 24\ 25\ 11\ 14\ 18\ 22\ 2\ 29\ 23\ 26\ 20\ 21\ 17\ 5\ 15\ 1\ 30\ )(6\ 12\ 19\ 28\ 3)(7\ 16\ 31\ 4).$$

This consists of periodic orbits of length $4, 5$ and 22. Now suppose we have $s = 5$ and have the s-subset $S = \{3, 8, 10, 14, 30\}$. This corresponds to the s-permutation with orbit notation given by

$$[13\ 27\ 9\ 8][10][24\ 25\ 11\ 14][18\ 22\ 2\ 29\ 23\ 26\ 20\ 21\ 17\ 5\ 15\ 1\ 30][6\ 12\ 19\ 28\ 3](7\ 16\ 31\ 4).$$

Now we have singular orbits of length $1, 4, 5, 5, 12$ and a periodic orbit of length 5. In a directed graph representation of the permutation $\hat{f}$, this construction can be seen as "cutting" or removing s edges corresponding to the vertices of the s-subset. This is shown in figure 4.1 for the above example on 31 points where the cycles are shown for the permutation on 31 points and the corresponding s-permutation by ignoring the directed edges coloured red.

Let f be a permutation and suppose an s-subset is chosen. From the previous example, the following should be clear.

1. Any cycle not containing a singular point or an origin point is retained in the s-permutation. Let l be the number of cycles retained.

2. There are s orbits of the s-permutation each starting with an origin point and ending with a singular point.

3. The number of (periodic and singular) orbits of the s-permutation is $s + l$.

4.2 Combinatorial model for birational map

Let S and $\bar{S}$ be singular and origin sets respectively, so that $|S| = s = |\bar{S}|$. Let $W(N, s)$ be the set of all functions $f : [N] - S \to [N] - \bar{S}$.

Theorem 4.2.1. *The size of the set $W(N, s)$ is*

$$\#W(N, s) = \binom{N}{s}\binom{N}{s}(N - s)! = \binom{N}{s}N^{\underline{N-s}}. \tag{4.7}$$

where $n^{\underline{k}} = n(n-1)\dots(n-(k-1))$, the falling factorial.

Proof. The first term is the number of ways of choosing the s singular points, and the second term is the number of ways of choosing the s origin points. The third term is the number of ways of assigning the $N - s$ points with an image in a one-to-one manner since the first point has $N - s$ choices (points in $\bar{S}$ are unavailable to it) and the second point has $N - s - 1$ and so on. □

Theorem 4.2.2. *For fixed N and $0 \leq s < N$ every s-permutation on N points can be constructed in this way from exactly $s!$ distinct permutations.*

Proof. Suppose we are given an s-permutation and an associated $f : [N] - S \to [N]$. Consider the function $\bar{f} : [N] \to [N]$ where $\bar{f}(y) = f(y)$ for all $y \in [N] - S$. Now, the remaining $n \in S$ can be assigned in $|S|! = s!$ ways, and hence there are $s!$ permutations that contain the s-permutation. □

Corollary 4.2.3. *Picking an s-permutation on N points uniformly at random is equivalent to picking a random permutation on N points and a random s-subset and performing the construction in 4.1.11.*

This gives an intuitive way to think of s-permutations in a constructive way from permutations. Given a function f chosen uniformly at random in $W(N, s)$, we wish to find the expected statistics of its orbits. This will be used to model a birational map.

Theorem 4.2.4. *Let f be in $W(N,s)$ with parameters N, s. Let $\mathcal{S}_N(x)$ be the proportion of $[N]$ occupied by singular orbits with length less than or equal to $\frac{N}{s}x$. That is,*

$$\mathcal{S}_N(x) = \frac{\#\{z \in [N] \mid z \text{ belongs to a singular orbit}, t(z) \leq \frac{N}{s}x\}}{N} \tag{4.8}$$

where $t(z)$ is the length of the orbit of z. Also let $s(N)$ be the number of singular points as a function of N. Then if

$$\lim_{N\to\infty} s(N) = \infty \qquad \lim_{N\to\infty} \frac{s(N)}{N} = 0, \tag{4.9}$$

then for all $x \geq 0$, we have the limit $\mathcal{S}_N(x) \to \mathcal{R}(x) := 1 - e^{-x}(1+x)$. In addition, almost all points in $[N]$ belong to singular orbits.

This theorem states that if the number of singular points (and hence singular orbits) grows as number of points N grows, but at a slower rate, then the expected scaled length distribution of the singular orbits is the same as the distribution of all the orbits, and is given by $\mathcal{R}(x)$. This is the cumulative distribution function of the gamma distribution with shape and rate 2 and 1 respectively. Intuitively, the presence of singular points places a constraint on the points in space and in a large part governs most of the statistics. The proof of theorem 4.2.4 will follow after some preliminary results.

4.2.1 Distribution of singular orbits

Lemma 4.2.5. *For $0 < x < 1$ we have the inequality*

$$\frac{-x}{1-x} < \log(1-x) < -x. \tag{4.10}$$

This can also be proved easily using the mean value theorem by considering $f(t) = \log(1-t)$ on $[0, x]$.

Lemma 4.2.6. *Let k, s, N be integers with $0 \leq k < N$ and $0 \leq s < N$ and $k + s \leq N$. Then,*

$$e^{-\frac{sk}{N-k-s+1}} \leq \frac{(N-k)!(N-s)!}{N!(N-k-s)!} \leq e^{-\frac{sk}{N}} \tag{4.11}$$

with equality only if $s = 0$ or $k = 0$.

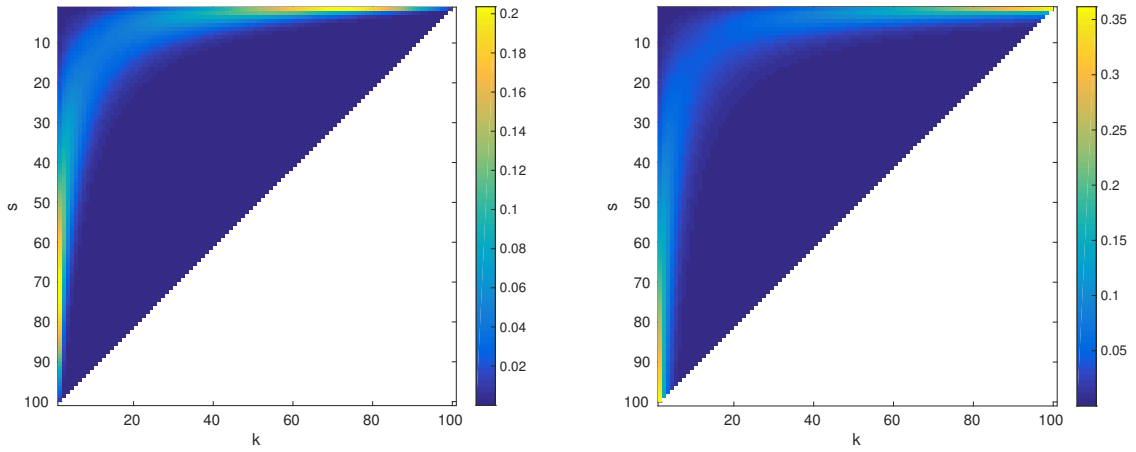


Figure 4.2: The error in the lower (left) and upper (right) bounds in equation (4.11) with $N = 100$ and $1 \leq k, s \leq 100$.

Proof. Note that this inequality is symmetric in s, k. For $s = 0$ or $k = 0$, we have equality as all three terms are 1. Now we consider all other values. We can write the factorials as the product

$$\frac{(N-k)!(N-s)!}{N!(N-k-s)!} = \prod_{j=0}^{k-1} \left(1 - \frac{s}{N-j}\right), \tag{4.12}$$

and clearly we have

$$\left(1 - \frac{s}{N-k+1}\right)^k \leq \prod_{j=0}^{k-1} \left(1 - \frac{s}{N-j}\right) \leq \left(1 - \frac{s}{N}\right)^k \tag{4.13}$$

with equality only when $k = 1$. Now focusing on the right hand term,

$$\left(1 - \frac{s}{N}\right)^k = \exp\left[k \log\left(1 - \frac{s}{N}\right)\right] < \exp\left(\frac{-sk}{N}\right) \tag{4.14}$$

since $\log(1-x) < -x$ for $0 < x < 1$ by lemma 4.2.5. Now for the left hand side, since $\log(1-x) > \frac{-x}{1-x}$ the result follows immediately using the same method.

□

Figure 4.2 shows the errors for the lower and upper bounds in equation (4.11). We see that the error is small for medium sized values of s, k. We now prove theorem 4.2.4 by constructing and counting the number of singular k-orbits and finding their distribution. Note that a singular orbit consists of exactly one origin point and one singular point.

Proof. (Theorem 4.2.4) Let us count the number of singular k-orbits. Then $(x_1, x_2, \ldots, x_k)$ is the required k-arc where $x_1 \in \bar{S}, x_k \in S$. The number of these k-arcs is $N^{\underline{k}}$. They occur with multiplicity determined by the reduced space with $N-k$ points and $s-1$ singular points,

$$\#W(N-k, s-1) = \binom{N-k}{s-1}(N-k)^{\underline{s-1}} \tag{4.15}$$

Let the average of P_k^s with respect to the uniform probability on W be denoted by $\langle P_k^s \rangle$. Then the average value of P_k^s (the space consumed by singular k-orbits) is

$$\begin{aligned}
\langle P_k^s \rangle &= \frac{k}{N} N^{\underline{k}} \frac{\#W(N-k, s-1)}{\#W(N, s)} && (4.16)\\
&= \frac{s^2 k}{N} \frac{(N-s)^{\underline{k-1}}}{N^{\underline{k}}} && (4.17)\\
&= \frac{s^2 k}{N(N-k+1)} \prod_{j=0}^{k-1} \left(1 - \frac{s}{N-j}\right). && (4.18)
\end{aligned}$$

Now let x be a positive real number. We consider the proportion of space consumed in singular orbits of length less than or equal to x, that is, the sum of (4.18) from $k=1$ to $\lfloor x \rfloor$. Using (4.12) and summing, this can be shown to be

$$\sum_{k=1}^{\lfloor x \rfloor} \langle P_k^s \rangle = 1 - \frac{N-s}{N(s+1)} - \left(1 - \frac{1}{s}\right)\left(1 + \frac{\lfloor x \rfloor\, s}{N} + \frac{1}{N}\right) \frac{(N-\lfloor x \rfloor)!(N-s)!}{N!(N-s-\lfloor x \rfloor)!}. \tag{4.19}$$

Now we apply Lemma 4.2.6 to obtain

$$\begin{aligned}
\sum_{k=1}^{\lfloor x \rfloor} \langle P_k^s \rangle &> 1 - \frac{N-s}{N(s+1)} - \left(1 - \frac{1}{s}\right)\left(1 + \frac{\lfloor x \rfloor\, s}{N} + \frac{1}{N}\right) e^{-\frac{\lfloor x \rfloor s}{N}}. && (4.20)\\
&= 1 - e^{-\frac{\lfloor x \rfloor s}{N}} \left(1 + \frac{\lfloor x \rfloor\, s}{N}\right) + O\left(\frac{1}{s}\right) && (4.21)
\end{aligned}$$

and

$$\begin{aligned}
\sum_{k=1}^{\lfloor x \rfloor} \langle P_k^s \rangle &< 1 - \frac{N-s}{N(s+1)} - \left(1 - \frac{1}{s}\right)\left(1 + \frac{\lfloor x \rfloor\, s}{N} + \frac{1}{N}\right) e^{-\frac{\lfloor x \rfloor s}{N-\lfloor x \rfloor - s + 1}}. && (4.22)\\
&= 1 - e^{-\frac{\lfloor x \rfloor s}{N-\lfloor x \rfloor - s + 1}} \left(1 + \frac{\lfloor x \rfloor\, s}{N}\right) + O\left(\frac{1}{s}\right). && (4.23)
\end{aligned}$$

Now suppose that $\lim_{N\to\infty} s(N) = \infty$ and $\lim_{N\to\infty} \frac{s(N)}{N} = 0$. Taking the limit as $N \to \infty$ and combining the inequalities we get the desired result

$$\sum_{k=1}^{\lfloor x \rfloor} \langle P_k^s \rangle = 1 - e^{-\frac{\lfloor x \rfloor s}{N}} \left(1 + \frac{\lfloor x \rfloor\, s}{N}\right). \tag{4.24}$$

□

This cumulative distribution is $\mathcal{R}(x)$, the gamma distribution with shape and rate 2 and 1 respectively, and shows that in the limit, all points belong to singular orbits as $\mathcal{R}(x) \to 1$ as $x \to \infty$. This shows that there is a universal scaled distribution for singular orbits in birational maps. This is the same distribution for the (symmetric) cycles in a reversible map as shown in [64]. This is interesting as these are two different types of maps. However, the manifestation of singular orbits for a birational map and the symmetric orbits in reversible maps is similar. For birational maps, singular orbits must start at an origin point and end at a singular point. This has a direct correspondence with the symmetric orbits in reversible maps which have a similar constraint with $\mathrm{Fix}(G)$ and $\mathrm{Fix}(H)$ which will be seen in the combinatorial model in chapter 8.

4.2.2 Periodic orbits and points

In this subsection we consider the expected value for the number of periodic orbits, and the number of points belonging to periodic orbits. Recall a periodic point is a point belonging to a periodic orbit. We first provide a lemma which calculates a summation which we will encounter later.

Lemma 4.2.7. *For positive integers N, s with $0 \le s < N$ we have that*

$$\sum_{k=1}^{N-s} \frac{(N-k)!(N-s)!}{N!(N-s-k)!} = \sum_{k=1}^{N-s} \prod_{j=0}^{k-1} \left(1 - \frac{s}{N-j}\right) \tag{4.25}$$

$$= \frac{N-s}{s+1}. \tag{4.26}$$

Proof. Let s be fixed and let

$$\sigma_N = \sum_{k=1}^{N-s} \prod_{j=0}^{k-1} \left(1 - \frac{s}{N-j}\right). \tag{4.27}$$

Then by taking out the common factor corresponding to the $j = 0$ term, we have

$$\begin{aligned}
\sigma_N &= \left(1 - \frac{s}{N}\right)\left[1 + \sum_{k=2}^{N-s}\prod_{j=1}^{k-1}\left(1 - \frac{s}{N-j}\right)\right] \\
&= \left(1 - \frac{s}{N}\right)\left[1 + \sum_{k=2}^{N-s}\prod_{j=0}^{k-2}\left(1 - \frac{s}{N-1-j}\right)\right] \qquad \text{(re-indexing)} \\
&= \left(1 - \frac{s}{N}\right)\left[1 + \sum_{k=1}^{N-1-s}\prod_{j=0}^{k-1}\left(1 - \frac{s}{N-1-j}\right)\right] \qquad \text{(re-indexing)} \\
&= \left(1 - \frac{s}{N}\right)(1 + \sigma_{N-1}).
\end{aligned}$$

This gives us the recurrence relation

$$\sigma_N = \left(1 - \frac{s}{N}\right)(1 + \sigma_{N-1}), \tag{4.28}$$

which has solution

$$\sigma_N = \frac{N-s}{s+1}. \tag{4.29}$$

This can be derived using standard methods for ordinary generating functions. □

Another question of interest is the number of periodic orbits. From corollary 4.2.3, it is clear that the expected number of periodic orbits must be less than the expected number in a random permutation, H_N.

Theorem 4.2.8. *For fixed N and $0 \leq s < N$, the expected number of periodic orbits is given by*

$$\langle \#cycles \rangle = H_N - H_s, \tag{4.30}$$

where H_n is the nth harmonic number and $H_0 = 0$ (see (3.3)).

This result is also valid for the degenerate case $s = N$ which will have no periodic orbits as all points are singular orbits of length one. A proof of this theorem follows below. For $s = 0$, this reverts to the case of a random permutation and this result is well known and given in theorem 3.1.3.

Proof. For $0 \leq s < N-1$, let us consider the number of k-cycles. The k-arc required here is $(x_1, x_2, \ldots, x_k)$ where none of x_i are in S or $\bar{S}$. The number of these is $N^{\underline{k}}/k$. They

occur with multiplicity determined by the reduced space with $N-k$ points and s singular points. So the average number of k-cycles is given by

$$\langle \#k\text{-cycles} \rangle = \frac{1}{k} N^{\underline{k}} \frac{\#W(N-k,s)}{\#W(N,s)} \tag{4.31}$$

$$= \frac{1}{k} \frac{(N-k)!(N-s)!}{N!(N-s-k)!}. \tag{4.32}$$

Note that for $k > N-s$, we have $\langle \#k\text{-cycles} \rangle = 0$ since there are at most $N-s$ points in a periodic orbit. Now consider the sum over k,

$$\langle \#\text{cycles} \rangle = \sum_{k=1}^{N-s} \langle \#k\text{-cycles} \rangle \tag{4.33}$$

$$= \sum_{k=1}^{N-s} \frac{1}{k} \frac{(N-k)!(N-s)!}{N!(N-s-k)!}. \tag{4.34}$$

Now let $P(s)$ be the statement

$$\sum_{k=1}^{N-s} \frac{1}{k} \frac{(N-k)!(N-s)!}{N!(N-s-k)!} = H_N - H_s. \tag{4.35}$$

We prove that $P(s)$ is true by for $0 \leq s < N$ by induction. First for $s = 0$ on the left hand side of $P(0)$ we have

$$\sum_{k=1}^{N} \frac{1}{k} \frac{(N-k)!N!}{N!(N-k)!} = \sum_{k=1}^{N} \frac{1}{k} = H_N = H_N - H_0, \tag{4.36}$$

so $P(0)$ is true. Let $0 \leq t < N-1$. Now assume $P(t)$ is true, we will show that $P(t+1)$ is true. Consider the left hand side of $P(t+1)$, so we have

$$\sum_{k=1}^{N-t-1} \frac{1}{k} \frac{(N-k)!(N-t-1)!}{N!(N-t-1-k)!} \tag{4.37}$$

$$= \sum_{k=1}^{N-t-1} \frac{1}{k} \frac{(N-k)!(N-t)!}{N!(N-t-k)!} \frac{N-t-k}{N-t} \tag{4.38}$$

$$= \sum_{k=1}^{N-t-1} \frac{1}{k} \frac{(N-k)!(N-t)!}{N!(N-t-k)!} \left(1 - \frac{k}{N-t}\right) \tag{4.39}$$

$$= \sum_{k=1}^{N-t-1} \frac{1}{k} \frac{(N-k)!(N-t)!}{N!(N-t-k)!} - \frac{1}{N-t} \sum_{k=1}^{N-t-1} \frac{(N-k)!(N-t)!}{N!(N-t-k)!}, \tag{4.40}$$

and using (4.35) and lemma 4.2.7

$$=H_N - H_t - \frac{1}{N-t}\frac{s!(N-t)!}{N!} - \frac{1}{N-t}\left(\frac{N-t}{t+1} - \frac{s!(N-t)!}{N!}\right) \tag{4.41}$$

$$=H_N - H_t - \frac{1}{t+1} \tag{4.42}$$

$$=H_N - H_{t+1} \tag{4.43}$$

so $P(t+1)$ is true. Therefore, the statement $P(s)$ is true by induction for $0 \leq s < N$. □

Conjecture 4.2.9. *Let X be the number of periodic orbits in an s-permutation on N points. The variance is given by*

$$Var_{N,s}(X) = \left(H_N - \sum_{i=1}^{N}\frac{1}{i^2}\right) - \left(H_s - \sum_{i=1}^{s}\frac{1}{i^2}\right) = \sum_{i=s+1}^{N}\frac{1}{i} - \frac{1}{i^2}. \tag{4.44}$$

This is a statement on the variance on the number of periodic orbits. Indeed, it states that the variance is strictly less than the expected value. This has been verified numerically for small n, s $(1 \leq n \leq 7, 0 \leq s < n)$. This shows that the spread of the number of cycles is quite "nice".

Theorem 4.2.10. *The expected number of periodic points is given by*

$$\langle \#\textit{periodic points} \rangle = \frac{N-s}{s+1}. \tag{4.45}$$

Proof. Using (4.32), the number of periodic points belonging to periodic orbits of length k is given by

$$\langle \#k\text{-periodic points} \rangle = k\langle \#k\text{-cycles} \rangle \tag{4.46}$$

$$= \frac{(N-k)!(N-s)!}{N!(N-s-k)!}. \tag{4.47}$$

Thus summing over k, we have by lemma 4.2.7 the desired result. □

Corollary 4.2.11. *The proportion of periodic points is*

$$\frac{N-s}{N(s+1)} = \frac{1}{s+1} - \frac{1}{N} + \frac{1}{N(s+1)}, \tag{4.48}$$

which shows the proportion of periodic cycles is asymptotic to $\frac{1}{s+1}$ as N grows.

We may also be interested in the distribution of the periodic points.

Theorem 4.2.12. *Consider an s-permutation on N points with s singular points satisfying* (4.9)*. As* $N \to \infty$ *has scaled distribution* $1 - e^{-x}$*.*

Proof. The longest possible periodic orbit has length $N - s$. Now for $0 \leq x \leq N - s$, consider the number of points belonging to periodic orbits of length less than or equal to x, given by

$$\mathcal{D}_{per}(x) = \frac{1}{N} \sum_{k=1}^{\lfloor x \rfloor} \langle \#k\text{-periodic points} \rangle \tag{4.49}$$

$$= \frac{1}{N} \sum_{k=1}^{\lfloor x \rfloor} \frac{(N-k!)(N-s)!}{N!(N-s-k)!} \tag{4.50}$$

$$= \frac{1}{N} \left(\frac{N-s}{s+1} - \frac{(N-s)!(N-\lfloor x \rfloor)!}{(s+1)N!(N-s-\lfloor x \rfloor)!} (N-s-\lfloor x \rfloor) \right). \tag{4.51}$$

Now we apply Lemma 4.2.6 to yield

$$\frac{N-s}{N(s+1)} \left(1 - e^{-\frac{(s+1)\lfloor x \rfloor}{N}} \right) < \mathcal{D}_{per}(x) < \frac{N-s}{N(s+1)} \left(1 - e^{-\frac{(s+1)\lfloor x \rfloor}{N-\lfloor x \rfloor - s}} \right). \tag{4.52}$$

Now supposing the conditions in (4.9) and taking the limit as $N \to \infty$ we get

$$\mathcal{D}_{per}(x) = \frac{N-s}{N(s+1)} \left(1 - e^{-\frac{(s+1)\lfloor x \rfloor}{N}} \right), \tag{4.53}$$

and we have the desired result with scaling factor $(s+1)/N$. □

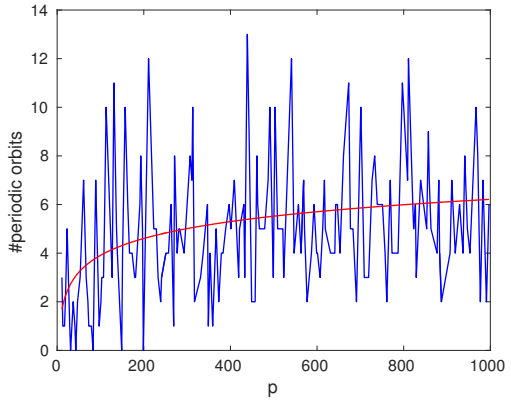
4.3 Model vs birational maps

In this section, we compare the expected values calculated in the previous section using the combinatorial model with the observed values in various birational maps. Consider a general birational map over $\mathbb{F}_p^2$ given by

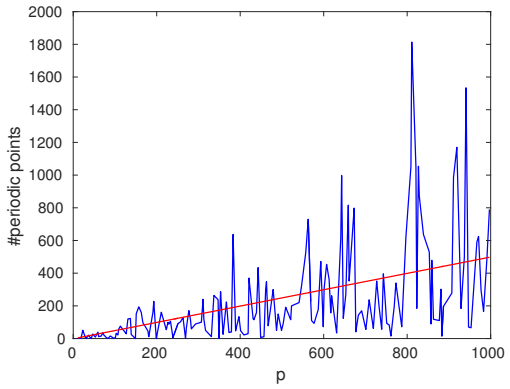
$$L : x' = y, \qquad y' = \frac{f_1(y)x + f_2(y)}{f_3(y)x + f_4(y)}, \tag{4.54}$$

where f_i are polynomials and $f_3(y)x + f_4(y) \neq 0$ and $f_2(x)f_3(x) - f_4(x)f_1(x) \neq 0$. This is invertible with inverse given by

$$L^{-1} : x' = \frac{f_2(x) - yf_4(x)}{yf_3(x) - f_1(x)}, \qquad y' = x. \tag{4.55}$$



(a) Number of periodic orbits in the birational map L_1 in example 4.3.1 with $(a, b, c, d) = (4, 1, 3, 2)$ for $p = 11, \ldots, 997$ compared with the expected value (4.30).



(b) Number of periodic points in the birational map L_1 in example 4.3.1 with $(a, b, c, d) = (4, 1, 3, 2)$ for $p = 11, \ldots, 997$ compared with the expected value (4.45).

Figure 4.3

We can further simplify this map with the following 2 examples.

Example 4.3.1. Consider the birational map L_1 over $\mathbb{F}_p^2$

$$L_1 : x' = y, \qquad y' = x + \frac{f(y)}{g(y)}, \qquad g(y) \neq 0. \tag{4.56}$$

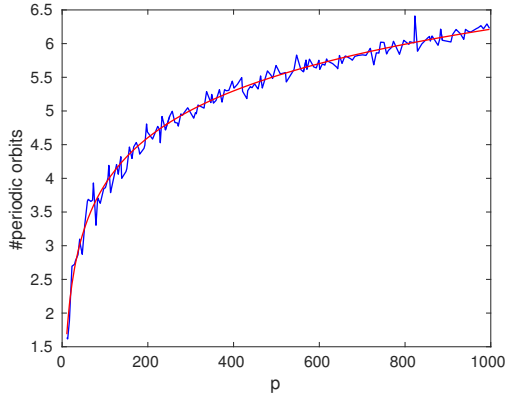
This has inverse L_1^{-1} given by

$$L_1^{-1} : x' = y - \frac{f(x)}{g(x)}, \qquad y' = x, \qquad g(x) \neq 0. \tag{4.57}$$

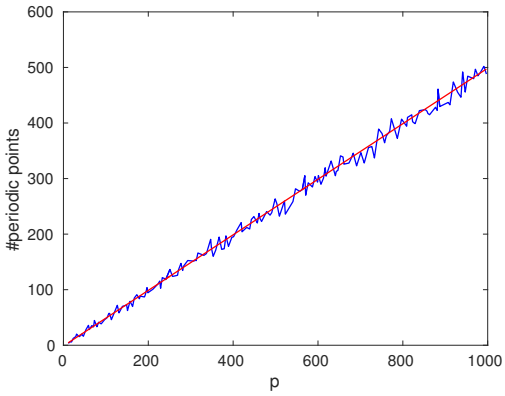
For example, let f be the general cubic $f(x) = ax^3 + bx^2 + cx + d$, and g be the quadratic $g(x) = (2x + 1)(x + 1)$. The singular points of L_1 are where $g(y) = 0$, that is, all points with y-coordinate -1 or -2^{-1} modulo p. Thus, for a fixed p, there are $2p$ singular points (and $2p$ origin points) since x is arbitrary and hence $2p$ singular orbits. The number of periodic orbits and points is shown in figure 4.3 compared to the expected values given in (4.30) and (4.45) with $N = p^2$ and $s = 2p$. Once we introduce averaging over parameter values δ, we obtain excellent agreement as per figure 4.4. Figure 4.5 shows the distribution of the singular orbits for $p = 997$ compared with $\mathcal{R}(x)$ as discussed in theorem 4.2.4.

Example 4.3.2. Consider the birational map L_2 over $\mathbb{F}_p^2$

$$L_2 : x' = y, \qquad y' = \frac{x + f(y)}{g(y)}, \qquad g(y) \neq 0 \tag{4.58}$$



(a) Number of periodic orbits in the birational map L_1 in example 4.3.1 with $(a, b, c, d) = (4, 1, 3, \delta)$ for $p = 11, \ldots, 997$ averaged over $\delta = 0 \ldots p-1$ compared with the expected value (4.30).



(b) Number of periodic points in the birational map L_1 in example 4.3.1 with $(a, b, c, d) = (4, 1, 3, \delta)$ for $p = 11, \ldots, 997$ averaged over $\delta = 0 \ldots p-1$ compared with the expected value (4.45).

Figure 4.4

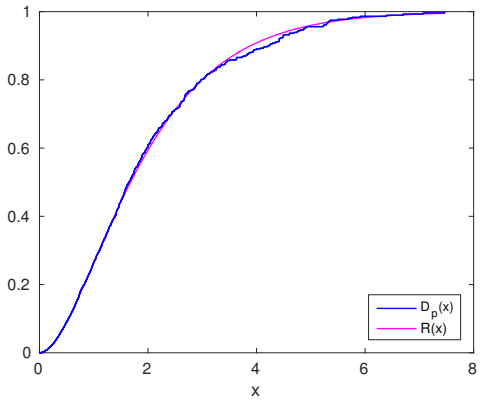
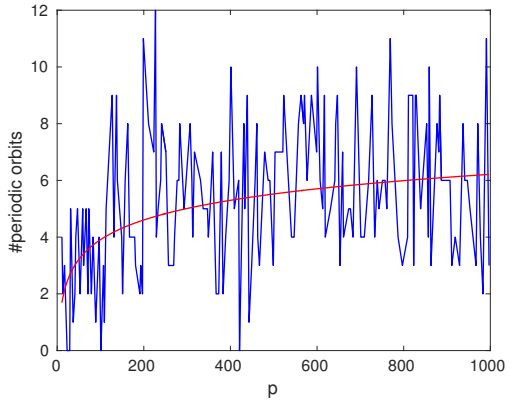


Figure 4.5: Distribution of the scaled lengths of singular orbits for the birational map L_1 compared with $\mathcal{R}(x)$ with $p = 997$ with parameters $(a, b, c, d) = (4, 1, 3, 2)$.

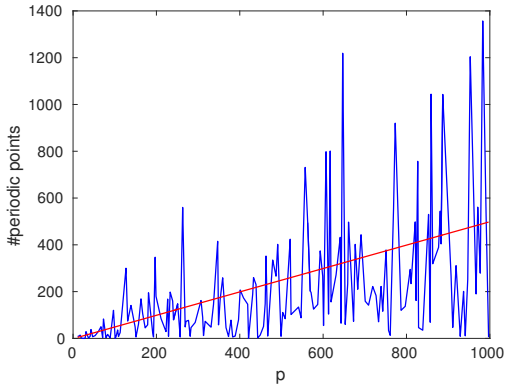
with inverse map L_2^{-1} given by

$$L_2^{-1} : x' = g(x)y - f(x), \qquad y' = x, \qquad g(x) \neq 0. \tag{4.59}$$

We use the same polynomials f and g as in the previous example. Figure 4.6 compares the number of periodic orbits and points in L_2 compared with the expected number from (4.30) and (4.45) respectively with $N = p^2$ and $s = 2p$. Again, we see that once we average over parameter δ as in figure 4.7 we obtain an excellent agreement. Figure 4.8 shows the distribution of the lengths of singular orbits for $p = 997$ compared with $\mathcal{R}(x)$ as discussed in theorem 4.2.4.

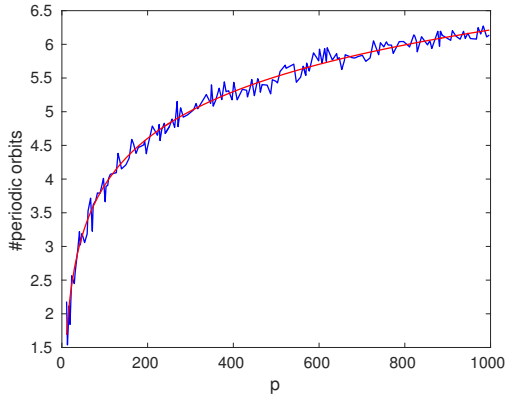


(a) Number of periodic orbits in the birational map L_2 in example 4.3.2 with $(a, b, c, d) = (4, 1, 3, 2)$ for $p = 11, \ldots, 997$ compared with the expected value (4.30).

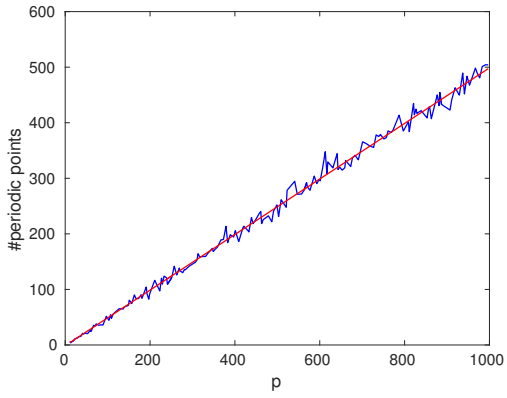


(b) Number of periodic points in the birational map L_2 in example 4.3.2 with $(a, b, c, d) = (4, 1, 3, 2)$ for $p = 11, \ldots, 997$ compared with the expected value (4.45).

Figure 4.6



(a) Number of periodic orbits in the birational map L_2 in example 4.3.2 with $(a, b, c, d) = (4, 1, 3, \delta)$ for $p = 11, \ldots, 997$ averaged over $\delta = 0 \ldots p-1$ compared with the expected value (4.30).



(b) Number of periodic points in the birational map L_2 in example 4.3.2 with $(a, b, c, d) = (4, 1, 3, \delta)$ for $p = 11, \ldots, 997$ averaged over $\delta = 0 \ldots p-1$ compared with the expected value (4.45).

Figure 4.7

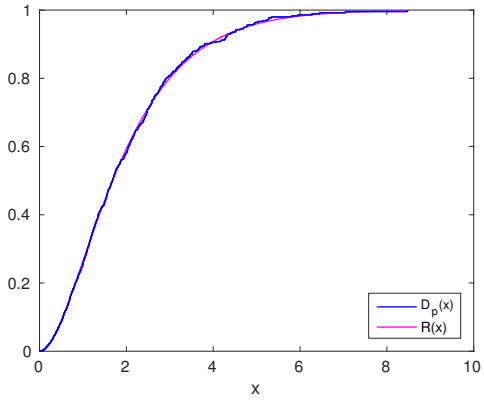


Figure 4.8: Distribution of the scaled lengths of singular orbits for the birational map L_2 compared with $\mathcal{R}(x)$ with $p = 997$ with parameters $(a, b, c, d) = (4, 1, 3, 2)$.

4.4 Concluding remarks

This whole chapter is entirely original work and the results and ideas are quite general. It can be seen as an extension of the statistics of random permutations. We constructed and derived a model for s-permutations on n points, an analog to that of random permutations in chapter 3, but allowing for singular points. We did this by evaluating the expected value for various cycle statistics of all functions on N points with s singular points. Now along with periodic orbits as before, we also have singular orbits which are constrained by the parameter for the number of singular points s. A main result obtained is the expected number of cycles which was shown to be $H_N - H_s$. We also considered the (scaled) distribution of the singular orbits which was shown to be the Gamma distribution. This will be seen again when we consider reversible maps in later chapters.

We also considered two specific examples of birational maps and saw that the expected statistics of an s-permutation corresponds closely with the observed statistics for these maps. This is similar to the case for random permutations and polynomial automorphisms. It appears that this combinatorial model is very effective as a model for the number of cycles in birational maps and seems like a good way for eliciting the behaviour of birational maps. We will see similar ideas used again in chapter 8 to great effectiveness. Note that we only expect this behaviour for birational maps that have no structural constraints or constraining properties. We will consider some special birational maps that are reversible and have integrals in the following chapters.

Chapter 5

Reversibility and its effect over finite fields

5.1 Introduction

In this chapter, we consider a large class of maps having the property *reversibility*. The origin of this can be traced back to the classical concept of time reversal symmetry in mechanics which is a property of invariance of dynamics under the transformation $t \mapsto -t$ and reversal of velocities [40]. Many physical laws exhibit this and it essentially means a system evolves the same if we look at it with time reversed. Devaney [17] generalised this idea of time reversal symmetry for dynamical systems to any involution (not just $t \mapsto -t$) with the following definition.

Definition 5.1.1. A dynamical system is *reversible* if there is an involution in phase space which reverses the direction of time.

5.2 Reversibility and dynamical consequences

We focus here on reversible maps. For reversible maps on finite fields, we are interested in the orbit statistics: the number, length, and distribution of the lengths of their orbits. Recall, that the mapping L on a space S is a rule that defines the next point our system,

$$z' = Lz \tag{5.1}$$

for $z \in S$. Then we have that a mapping L is reversible if there exists an involution G such that

$$L \circ Gz' = Gz, \tag{5.2}$$

which says that the action of G reverses the direction of our mapping in the sense that Gz is obtained from applying the mapping to Gz'. This is shown using a diagram in figure

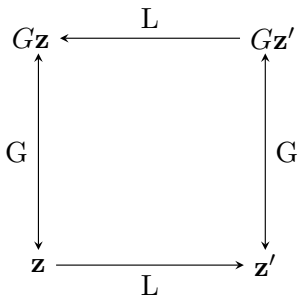


Figure 5.1: Arrow diagram showing the relationship in (5.2) of the action of the involution G and the mapping L.

5.1. By combining (5.1) and (5.2) we obtain

$$L \circ G \circ Lz = Gz \tag{5.3}$$

or

$$L \circ G \circ L = G \tag{5.4}$$

since this holds for arbitrary $z \in S$. We can also write L as the composition of two involutions H, G

$$L = H \circ G, \tag{5.5}$$

where $H = L \circ G$ is an involution since

$$H^2 = (L \circ G) \circ (L \circ G) = (L \circ G \circ L) \circ G = G^2 = Id. \tag{5.6}$$

The inverse mapping L^{-1} can be written as

$$L^{-1} = G \circ H, \tag{5.7}$$

and it is clear that this is well defined since $L \circ L^{-1} = (H \circ G) \circ (G \circ H) = I = (G \circ H) \circ (H \circ G) = L^{-1} \circ L$.

5.2.1 Symmetric and asymmetric orbits

For a reversible mapping, we can classify orbits as symmetric or asymmetric. For L written as (5.5), we call H and G reversing symmetries. The orbit of z, denoted as $\sigma(z)$,

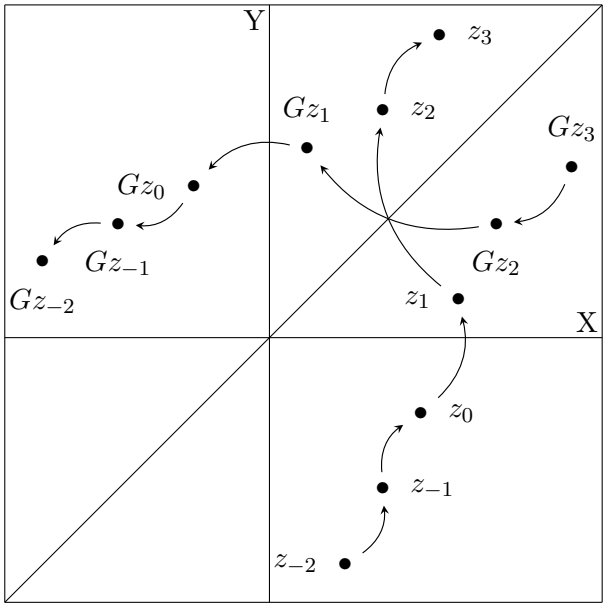


Figure 5.2: Figure showing the effect of a reversing symmetry $G : x' = y,\ y' = x$ in the plane. Notice the direction of the arrows in the reflected orbit showing the reversing action of G.

is symmetric with respect to G if it is invariant under G, that is,

$$G \circ \sigma(z) = \sigma(z), \tag{5.8}$$

and similarly for H. Note that symmetry with respect to one reversing symmetry implies the other. An orbit that is not invariant under H or G is called *asymmetric*. The fixed sets of H, G defined as

$$\mathrm{Fix}(H) = \{z \mid Hz = z\}, \qquad \mathrm{Fix}(G) = \{z \mid Gz = z\} \tag{5.9}$$

play an important role in the dynamics of the mapping L. We will call these the symmetry sets. The results in the rest of this section are well known and standard (e.g. see [40]).

Proposition 5.2.1. An orbit is symmetric if and only if it intersects a symmetry set.

Proof. Suppose that z belongs to a symmetric orbit (under G). Then,

$$Gz = L^i z \tag{5.10}$$

for some $i \in \mathbb{Z}$. If i is even, then using the identity $L^{-n} \circ G = G \circ L^n$ we get

$$G \circ L^{i/2} z = L^{i/2} z, \tag{5.11}$$

showing that the orbit intersects $\mathrm{Fix}(G)$. If i is odd, then

$$L \circ G \circ L^{(i+1)/2} z = L^{(i+1)/2} z, \tag{5.12}$$

and since $H = L \circ G$ we have

$$H \circ L^{(i+1)/2} z = L^{(i+1)/2} z, \tag{5.13}$$

which shows the orbit intersects $\mathrm{Fix}(H)$. Conversely, suppose an orbit intersects a symmetry set for G at z. Then we have $Gz = z$ and so

$$L^{-i} \circ Gz = L^{-i} z, \tag{5.14}$$

and using the identity $L^{-n} \circ G = G \circ L^n$ we get

$$G \circ L^i z = L^{-i} z, \tag{5.15}$$

showing that the orbit of z is symmetric as it is invariant under G. □

Corollary 5.2.2. *An asymmetric orbit does not intersect a symmetric set of L.*

This follows directly from theorem 5.2.1.

Corollary 5.2.3. *Asymmetric orbits come in pairs under G.*

Proof. Let z belong to an asymmetric orbit denoted by $\sigma(z)$. Since it is asymmetric, then it does not intersect a symmetric set of L by corollary 5.2.2. Thus, the orbit $\sigma(Gz)$ is distinct from $\sigma(z)$ and is also asymmetric (since $G^2 z = z$). Note that we do indeed only get pairs and not any more by the involution H because $\sigma(Gz) = \sigma(Hz)$. □

Proposition 5.2.4. Let $\sigma(z)$ be a symmetric periodic orbit, then $\sigma(z)$ intersects $\mathrm{Fix}(G) \cup \mathrm{Fix}(H)$ in two distinct points unless it is a fixed point in which case it belongs to both $\mathrm{Fix}(G)$ and $\mathrm{Fix}(H)$. In particular, if

- $\sigma(z)$ has even period $2k$, it either has two points z_1, z_2 in either $\mathrm{Fix}(G)$ or $\mathrm{Fix}(H)$ and $L^k z_1 = z_2$.
- $\sigma(z)$ has odd period $2k + 1$, it has a point $z_1 \in \mathrm{Fix}(G)$ and $z_2 \in \mathrm{Fix}(H)$ and $L^k z_1 = z_2$.

5.2.2 Necessary conditions for reversibility

Proposition 5.2.5. Suppose $L : \mathbb{C}^d \to \mathbb{C}^d$ is a reversible map and z_0 is a symmetric fixed point of L, that is, $Lz_0 = z_0$ and $Gz_0 = z_0$, then $det(J_L z_0) = \pm 1$.

Proof. Since L is reversible, we have $L \circ G \circ L = G$. Now finding the Jacobian matrix of both sides

$$J_L \circ (G \circ Lz)(J_G \circ (Lz))J_L(z) = J_G(z). \tag{5.16}$$

Now with $z = z_0$ and simplifying we have

$$J_L(z_0)J_G(z_0)J_L(z_0) = J_G(z_0). \tag{5.17}$$

Computing the determinant of both sides, we get

$$\det(J_L(z_0)) \det(J_G(z_0))det(J_L(z_0)) = \det(J_G(z_0)), \tag{5.18}$$

and since $\det(J_G(z)) \neq 0$ by the inverse function theorem,

$$\det(J_L(z_0))^2 = 1 \tag{5.19}$$

$$\implies \det(J_L(z_0)) = \pm 1. \tag{5.20}$$

□

Note that since each point of a k-cycle is fixed by L^k, which is also a reversible map, for the Jacobian determinant of a periodic point z_0 with period k we have $\det(J_{L^k}(z_0)) = \pm 1$ also.

Proposition 5.2.6. Suppose $L : \mathbb{C}^d \to \mathbb{C}^d$ is a reversible map and z_0 is an asymmetric fixed point of L, that is, $Lz_0 = z_0$ and $Gz_0 \neq z_0$. If $J_L(z_0)$ has eigenvalue λ, then $J_L(Gz_0)$ (the asymmetric partner for z_0) has eigenvalue λ^{-1}.

Lemma 5.2.7. *For invertible maps $M : \mathbb{C}^d \to \mathbb{C}^d$ we have that $J_{M^{-1}}(Mz)$ is the inverse of $J_M(z)$.*

Proof. By applying the Jacobian matrix we have

$$M^{-1}Mz = z \implies J_{M^{-1}}(Mz)J_M(z) = I \tag{5.21}$$

as required. □

Proof. (Proposition 5.2.6) Since L is reversible, we have $L^{-1} = G \circ L \circ G^{-1}$. Now finding the Jacobian matrix of both sides,

$$J_{L^{-1}}(y) = J_G(LG^{-1}y)J_L(G^{-1}y)J_{G^{-1}}(y). \tag{5.22}$$

Putting $y = Gz_0$,

$$J_{L^{-1}}(Gz_0) = J_G(LG^{-1}Gz_0)J_L(G^{-1}Gz_0)J_{G^{-1}}(Gz_0) \tag{5.23}$$

$$= J_G(Lz_0)J_L(z_0)J_{G^{-1}}(Gz_0) \tag{5.24}$$

$$= J_G(z_0)J_L(z_0)J_{G^{-1}}(Gz_0). \tag{5.25}$$

Now applying lemma 5.2.7 we can write

$$J_{L^{-1}}(Gz_0) = PJ_L(z_0)P^{-1}, \tag{5.26}$$

where $P = J_G(z_0)$. This tells us that $J_{L^{-1}}(Gz_0)$ has the same eigenvalues as $J_L(z_0)$. Now applying lemma 5.2.7 with $M = L$ and $z = L^{-1}Gz_0$ we get that

$$J_{L^{-1}}(Gz_0)J_L(Gz_0) = I, \tag{5.27}$$

since $L^{-1} \circ Gz_0 = G \circ Lz_0 = Gz_0$. In particular, $J_{L^{-1}}(Gz_0)$ has reciprocal eigenvalues to $J_L(Gz_0)$, and thus, $J_L(z_0)$ has reciprocal eigenvalues to $J_L(Gz_0)$.

□

Note that by definition if z_0 is an asymmetric fixed point, then Gz_0 is also an asymmetric fixed point. Proposition 5.2.5 and proposition 5.2.6 give necessary conditions for fixed points of a reversible mapping. This can be used as a test to prove that a diffeomorphic map is not reversible, although it can not prove that a map is reversible, nor can it find the reversing symmetry. Nevertheless it is an effective method for many maps. We can simply find all the fixed points of the mapping, and if their Jacobian determinant is not ± 1 (that is, they are not symmetric), then we check their eigenvalues which must be in reciprocal pairs with another fixed point if the mapping is reversible. Given a diffeomorphism, an algorithm which may be able to eliminate the possibility of reversibility is as follows:

1. Find all fixed points of the mapping
2. Find the Jacobian determinants evaluated at the fixed points
3. If there are any fixed points with Jacobian determinants not equal to ± 1, find the eigenvalues of all of the Jacobians.
4. Check if there exist reciprocal eigenvalues for those fixed points with Jacobian determinants not equal to ± 1.

This algorithm becomes less useful for area-preserving maps of the plane that have $\det(J_L(z)) = 1$ for all z and one can at most conclude that some unpartnered fixed points are necessarily symmetric if the map is reversible. Determining whether area-preserving maps are reversible or not is subtle [40].

5.3 Reversible dynamics over finite fields

When we consider dynamics over finite fields, we are restricted to a finite space, and hence there are a finite number of orbits. An interesting problem is to find this number or provide bounds on it. We can immediately obtain bounds by using properties of symmetric points and orbits in proposition 5.2.4. Here we are considering reversible maps that are defined for the whole space (so there are no singular orbits) and hence gives a permutation over the finite space.

Corollary 5.3.1. *[63] If $L = H \circ G$ is reversible then*

$$\#\mathrm{Fix}(G) = \#SymOddCycles(L) + 2\#SymEvenCycles(L)_G, \tag{5.28}$$

$$\#\mathrm{Fix}(H) = \#SymOddCycles(L) + 2\#SymEvenCycles(L)_H. \tag{5.29}$$

and consequently

$$\#\mathrm{Fix}(H) + \#\mathrm{Fix}(G) = 2\#SymCycles(L). \tag{5.30}$$

The subscript G in equation (5.28) denotes the even length symmetric cycles that intersect $\mathrm{Fix}(G)$ (similarly for H). These equations hold because each symmetric odd cycle has

exactly one point on each symmetry line, while the symmetric even cycles have two points on a particular symmetry line by proposition 5.2.4 where we have used the basic fact that

$$\#\text{SymEvenCycles}(L) = \#\text{SymEvenCycles}(L)_G + \#\text{SymEvenCycles}(L)_H, \tag{5.31}$$

$$\#\text{SymCycles}(L) = \#\text{SymOddCycles}(L) + \#\text{SymEvenCycles}(L). \tag{5.32}$$

Proposition 5.3.2. We obtain the following bound on the number of cycles of L,

$$\frac{\#\text{Fix}(G) + \#\text{Fix}(H)}{2} = \#\text{SymCycles}(L) \leq \#\text{Cycles}(L) \tag{5.33}$$

This follows directly by corollary 5.3.1. In practice we will see that this bound is quite tight as asymmetric orbits are rare. This immediately gives us a lower bound for the number of cycles in a reversible map. It is natural later that we may want to consider the number of asymmetric orbits present and the proportion of space they occupy. We will consider this in detail in Chapter 8.

5.4 Reversible Hénon map

Recall from chapter 3, we considered the dissipative Hénon map in equation (3.15). One of the disallowed parameter values was for $\delta = 1$ since in that case, the map is reversible. This is what we now consider. The reversible Hénon map over $\mathbb{F}_p^2$ is given by

$$L : x' = y, \qquad y' = -x + y^2 + \epsilon, \tag{5.34}$$

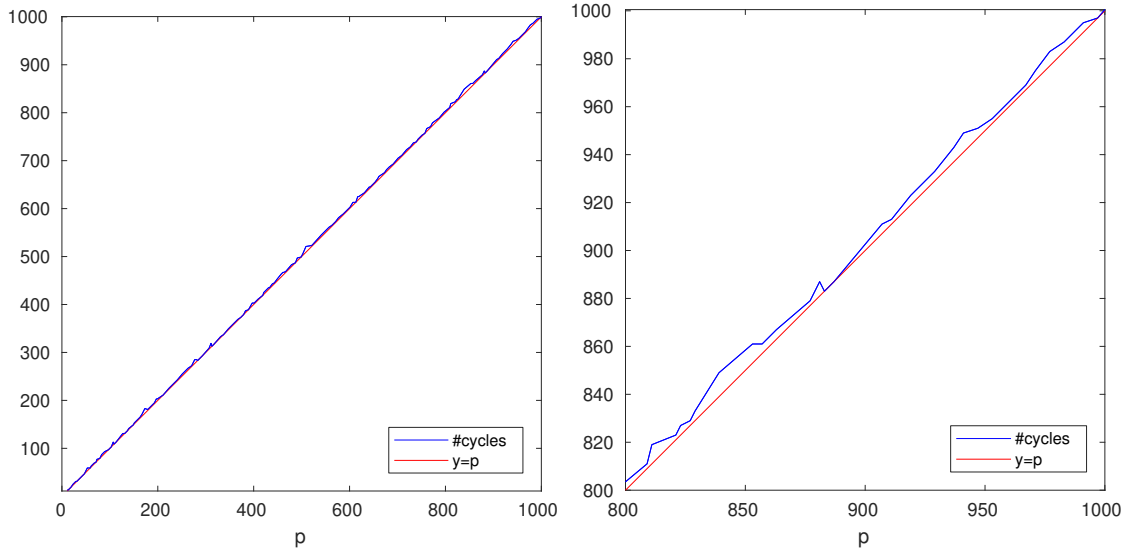
where $\epsilon \in \mathbb{F}_p$ and can be written as $L = H \circ G$ where H, G are involutions given by

$$H : x' = x,\ y' = -y + x^2 + \epsilon, \qquad G : x' = y,\ y' = x. \tag{5.35}$$

Consider the fixed sets of the involutions (for $p > 2$),

$$\text{Fix}(H) = \left\{ \left(x, \frac{x^2 + \epsilon}{2} \right) \middle| x \in \mathbb{F}_p \right\}, \qquad \text{Fix}(G) = \{(x, x) \mid x \in \mathbb{F}_p\}, \tag{5.36}$$

both with cardinality p. Then, the number of symmetric cycles is $\frac{p+p}{2} = p$ and this immediately tells us that the total number of cycles must be at least p. For chosen



(a) (b)

Figure 5.3: The number of cycles for the reversible Hénon map over $\mathbb{F}_p^2$ with $\epsilon = 1$ compared to p for primes from 11 to 997 (left) and for primes 809 to 997 (right). Note that for each prime p, the number of cycles is $\geq p$.

prime p, we can count the number of cycles present which is shown in figure 5.3. We see that for the reversible Hénon map, this bound is quite tight, that is, most of the cycles are symmetric cycles, and furthermore that they take up most of the phase space. In [63], Roberts and Vivaldi conjectured that asymptotically, the (scaled) distribution of the symmetric cycles is $\mathcal{R}(x) = 1 - e^{-x}(1+x)$ and that the proportion of space they consume goes to 1. In addition, they showed in [64] that this was also the expected distribution for the composition of two involutions with mild constraints on the cardinality of the fixed sets. This contrasts with the orbits of the Hénon map on the real plane where symmetric orbits would be rare and asymmetric orbits should dominate [44].

For the reversible map the number of cycles is approximately p, while for the dissipative map the number of cycles is expected to be $H_{p^2} \approx 2 \log p$. Thus, if we compare the number of cycles of the reversible Hénon map (see figure 5.3) with the dissipative Hénon map both over $\mathbb{F}_p^2$ (see figure 3.2), we see that the number of cycles can be an indicator of some additional structure, for example, reversibility.

5.5 Concluding remarks

In this chapter, we introduced the concept of reversibility in the context of maps. Reversibility is a property that equips a map with two reversing symmetries giving it a

structure which the orbits must follow. This property also means that reversible maps are invertible (where well defined) which motivated us in the previous chapters to focus on polynomial automorphisms and birational maps which are invertible maps. Over the finite field, reversibility greatly changes the orbit statistics and in particular, we saw that since a cycle either has 0 or 2 points on the symmetry sets, we can obtain a lower bound on the number of cycles (at least for a reversible map with no singularities) by counting the total number of points on the symmetry sets. This is vastly different and greater than the number of cycles we observed in the maps in chapter 3 and 4 which were not reversible.

The rest of this thesis is mostly focusing on reversible maps. In chapter 6 we will consider some reversible maps which in addition have an integral. In chapter 7, we will focus on a specific example of a reversible map. In chapter 8, we will consider the problem of modelling the number of cycles in a birational reversible map. Furthermore, we will see that these statistics will be able to distinguish the number of integrals which will considered in chapter 9.

Chapter 6

Integrals of motion and their effect over finite fields

In this chapter, we consider a property of maps: possessing an integral of motion. We focus on how this manifests itself in the finite field, and in particular, the effect on the orbits of the dynamical system. We give a definition before considering examples of maps with integrals by extending the Hénon map and a birational map from earlier chapters. We then consider the most simple and natural example of linear maps in 2D. We end with a more interesting example, a family of QRT maps and provide a brief heuristic of the number of cycles for these maps.

6.1 Integrals of motion

A mapping L over the d-dimensional space K^d has an *integral* $I : K^d \to K$ if there exists a non-constant $I(z)$ such that

$$I(Lz) = I(z). \tag{6.1}$$

for all $z \in K^d$. In other words, I is invariant under the mapping. We are interested in particular in the case that L is birational and I is rational. Suppose $I(z) = k$, then we call this the level set with height k. All points on the same orbit lie on the same level set. A mapping may have more than one rational integral. Consider a mapping L with $j < d$ integrals

$$I_1, I_2, \ldots, I_j. \tag{6.2}$$

The j integrals are functionally independent if their gradient vectors $\{\nabla I_i \mid i = 1, \ldots, j\}$ span a j-dimensional subspace of K^d. For a point z, there will be a level set height associated with each integral say $I_1(z) = k_1, I_2(z) = k_2, \ldots I_j(z) = k_j$. It is clear that all points in the same orbit must have the same level set heights for each integral. Also,

the points that have the j-tuple of level set heights $\{k_1, k_2, \ldots k_j\}$ describe an algebraic variety given by the solution to the j equations: $\{z \in K^d \mid I_1 = k_1, I_2 = k_2, \ldots, I_j = k_j\}$. Generally speaking, a dynamical system is integrable if it possesses a sufficient number of integrals of motion. In classical mechanics, a dynamical system is called *integrable* if it possesses a Poisson or symplectic structure [30]. The task of finding out whether a mapping is "integrable" has been of interest to many and various methods have been developed to detect it [27]. Most commonly, discrete mappings are considered over $\mathbb{R}, \mathbb{C}, \mathbb{Q}$ but we note that the integrable definition (6.1) over these fields reduces to the finite field $\mathbb{F}_p$ if $I(z)$ is rational. One of the aims in this chapter is to develop a method to detect (the number of) rational integrals of motion by examining the cycle structure of map over the finite field. (For birational maps, (6.1) is valid wherever Lz is defined.)

6.2 Artificial integral construction

We introduce the idea of an integral by constructing an artificial integral for the dissipative Hénon map considered previously in (3.15) and the birational map L_1 in (4.3.1). To do this, we add a third dimension and assign it the value of a parameter in the 2D map. We will see how this naturally augments the number of cycles we see by a factor of p. This idea will be useful for general maps with an integral and will enable us to develop a basic test for integral detection.

6.2.1 Polynomial automorphism with integral

We modify the 2D Hénon dissipative map (3.15) by adding a third dimension and making the parameter ϵ a variable. Let us replace ϵ with z and define our mapping over $\mathbb{F}_p^3$

$$H\acute{e}non3D_{dis} : \; x' = y, \qquad y' = -\delta x + y^2 + z, \qquad z' = z \tag{6.3}$$

for $\delta \in \mathbb{F}_p, \delta \neq 0, 1$. This map is a polynomial automorphism and has the integral

$$I(x, y, z) = z. \tag{6.4}$$

Each level set is a horizontal slice of the xyz-space. In this way, for fixed δ we can view this as p copies of the dissipative Hénon map with the height of the level set corresponding to the height of the horizontal slice. Then it follows that the number of cycles in this mapping is the sum of the cycles of the dissipative Hénon map for each parameter ϵ. We

expect this to be p times the expected number for a single dissipative Hénon map which was shown in chapter 3 to be modelled by a random permutation with p^2 points. That is, the number of cycles for the map (6.3) would be expected to be

$$pH_{p^2} = p(2\log p + \psi) + O(1/p). \tag{6.5}$$

Similarly, we could construct a map with more integrals by adding parameters appropriately. For example, we could construct a $d > 2$ dimensional map with $d-2$ integrals and by extension, the number of cycles we would expect would be

$$p^{d-2}H_{p^2} = p^{d-2}(2\log p + \phi) + O(1/p^{d-2}). \tag{6.6}$$

By performing a variable transformation, we can warp the integral in (6.4) to appear more interesting although the cycle structure of the map is the same. For example, we can consider the invertible map

$$X = x,\ Y = y,\ Z = F(x,y) + z. \tag{6.7}$$

Written explicitly, the transformed map arising from (6.3) is given by

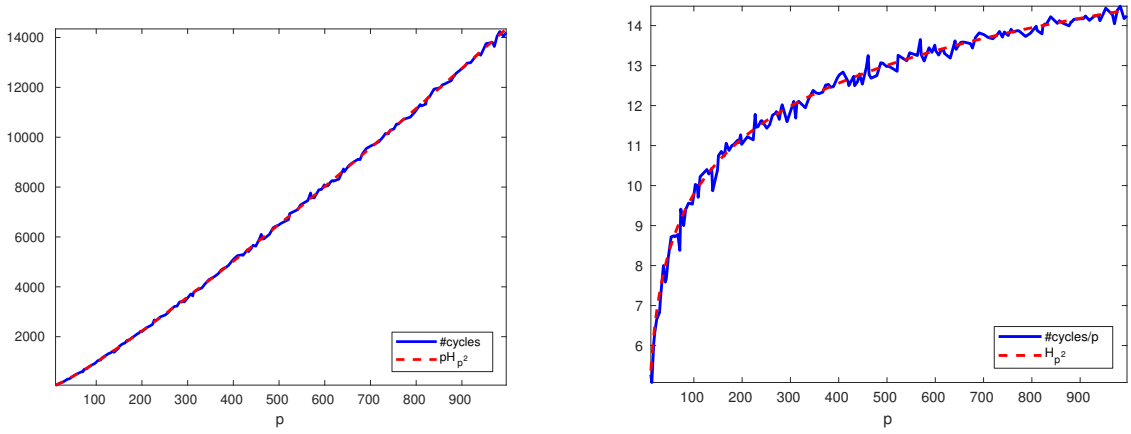
$$X' = Y, \qquad Y' = -\delta X + Y^2 + Z - F(X,Y), \qquad Z' = Z - F(X,Y) + F(X',Y') \tag{6.8}$$

with integral $I(X,Y,Z) = F(X,Y) - Z$. The cycle statistics of this mapping over $\mathbb{F}_p^3$ is the same as the map in (6.3) if we choose $F(x,y)$ to be polynomial. However given such a map it may not be obvious that it has such an integral. This idea can be generalised if we construct j integrals.

Suppose we have a mapping $\hat{L}$ which is a collection of p^j independent maps each acting on p^{d-j} points for a positive integer $j < d$. Note that $\hat{L}$ acts on $p^j p^{d-j} = p^d$ points. Then modelling each map as a random permutation using (3.3), the total number of cycles we expect is

$$N_c(\hat{L}) = p^j H_{p^{d-j}} = p^j \left[\log p^{d-j} + \phi + O\left(\frac{1}{p^{d-j}}\right)\right] \approx p^j(d-j)\log p. \tag{6.9}$$

We can think of $\hat{L}$ as a mapping with j integrals which partitions the space into p^j parts with each partition having the same number of points. For the above example,



(a) (b)

Figure 6.1: Number of cycles for the dissipative Hénon map in 3D (6.3) with $\delta = 2$ for primes $p = 11, \ldots, 997$ (left) and number of cycles divided by p (right).

we have $j = 1$ and figure 6.1 shows the number of cycles for this map compared to the probabilistic model for an ensemble of p random permutations of size p^2 which has approximately $p\log(p^2)$ cycles. This example shows a first idea of how an integral affects the number of cycles in a map.

To compare to the case of a map L of p^d points where we expect $N_c(L) = d\log p + \psi + O\left(\frac{1}{p^d}\right) \approx d\log p$, using (6.9) consider the ratio

$$\frac{N_c(\hat{L})}{N_c(L)} \approx p^j(1 - j/d) = O(p^j) \tag{6.10}$$

for fixed j, d. This shows that in the presence of the additional structure of an integral, we expect an increase of order p^j for the number of cycles. This shows that this may be used a test for the additional structure of an integral. For example, in figure 6.2 we see this being manifest.

This idea generalises to higher dimension, and when comparing maps that may both have integrals. Then we expect the ratio of the number of cycles to be $O(p^{j_1 - j_2})$ where j_1, j_2 are the number of integrals in the first and second map respectively.

6.2.2 Birational map with integral

We modify the birational map L_1 considered in example 4.3.1 with $f(x) = 4x^3 + x^2 + 3x + a$ and $g(x) = (2x+1)(x+1)$ and extend it to 3D. We let a be a variable and replace it with

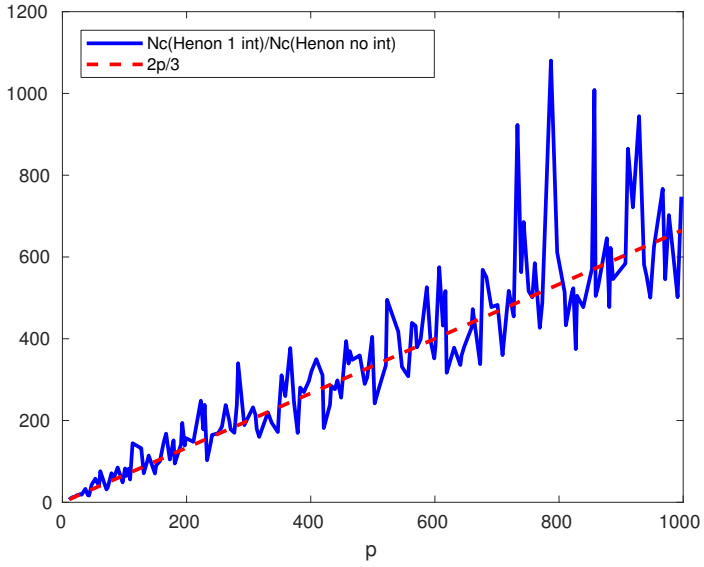


Figure 6.2: The ratio of number of cycles in (6.10) for the 3D Hénon map with 1 integral in (6.3) and the 3D Hénon map with no integral in (3.17) both with $\delta = 2$.

z to have the mapping over $\mathbb{F}_p^3$

$$L_1 : x' = y, \qquad y' = x + \frac{4y^3 + y^2 + 3y + z}{(2y+1)(y+1)}, \qquad z' = z \tag{6.11}$$

for $(2y+1)(y+1) \neq 0$. This is a birational map and like (6.4) has the integral $I(x, y, z) = z$. By an identical argument, we expect the number of cycles of

$$p(H_{p^3} - H_s), \tag{6.12}$$

where $s = 2p$ is the number of singular points. We do not provide a plot here as it would be identical to figure 4.4a with the the number of cycles and expected number multiplied by p.

We will examine how the above ideas may be used to identify the presence of integrals at the end of this chapter using a heuristic model. We note that in general, integrals are more exotic than in the constructed example above. For example, the number of points on level sets do not have to be the same as in (6.3). We will see an example of a 2D map with an integral where the level sets have varying number of points in section 6.4. However, there are algebraic bounds (Hasse-Weil bounds) which enable us to use similar arguments and ideas. We now move to a natural example of a map with an integral. These are linear maps for which the cycles exhibit very controlled behaviour which is at

one extreme of maps with an integral. The simplicity of the description allows for much information about the orbits to be solved algebraically.

6.3 Linear map with integral in 2D

The linear map in 2D is perhaps the most natural example to illustrate the effect of an integral over the finite space. We will see that we can say a lot about its dynamics and orbits over the finite field. Consider the matrix

$$A_\alpha = \begin{bmatrix} \alpha & -1 \\ 1 & 0 \end{bmatrix} \tag{6.13}$$

for $\alpha \in \mathbb{F}_p$. The matrix A_α has trace α and determinant 1. This induces the linear permutation mapping $f_\alpha : \mathbb{F}_p^2 \to \mathbb{F}_p^2$ given by $f_\alpha : (x', y')^T = A_\alpha (x, y)^T$ which can be written as

$$\begin{aligned} f_\alpha : x' &= \alpha x - y \\ y' &= x \end{aligned} \tag{6.14}$$

with inverse given by

$$\begin{aligned} f_\alpha^{-1} : x' &= y \\ y' &= \alpha y - x. \end{aligned} \tag{6.15}$$

This can be seen as the simplest one-parameter family of linear mappings. The mapping f_α has integral $I : \mathbb{F}_p^2 \to \mathbb{F}_p$ given by the quadratic form

$$I(x, y) = x^2 - \alpha xy + y^2. \tag{6.16}$$

This is easily verified by checking that $I(x', y') = I(x, y)$. Note that this map and corresponding integral is also well defined if considered over the real numbers. Each level set of this integral is a circle for $\alpha = 0$, an ellipse for $|\alpha| < 2$, a hyperbola for $|\alpha| > 2$, and a pair of lines for $\alpha = \pm 2$ (degenerate case). However, in the finite space, we lose all topology, for example, an ellipse doesn't "look like" a ellipse, and if we plot orbits of the mapping, it will be "hard" to see the presence of an integral. Of course, this is not a reliable way to spot an integral but shows even for simple integrals the possible difficulty in detection.

We now study the number of points on a level set of this linear map, and then we describe the possible cycle lengths of its orbits. We will see how the presence of an integral restricts and constrains these statistics. We note that the linear map induced by a general 2×2 matrices in $SL(2, \mathbb{Z})$ can also be studied with similar results but we consider the above example since we will consider a piece-wise linear map built from (6.14) in chapter 7.

6.3.1 Number of points on a level set

Consider some point (x_0, y_0) and suppose that $I(x_0, y_0) = k$ for some $k \in \mathbb{F}_p$. Since all points in the same orbit must lie on the same level set, the maximum length of the orbit of (x_0, y_0) is bounded by the number of points in $\mathbb{F}_p^2$ on the curve

$$x^2 - \alpha xy + y^2 = k \pmod{p}. \tag{6.17}$$

Baek et al. [4] found the number of points on a general conic over the finite space $\mathbb{F}_p^2$. They transformed the equation of the conic to simplify the equation to have only the x^2 and y^2 term. Using elementary number theory, they found that the number of solutions in this space depends on the quadratic residues of their coefficients modulo p. We demonstrate this idea with the integral of our linear mapping. Let

$$q(x, y) = x^2 - \alpha xy + y^2 - k \tag{6.18}$$

and define $q'(x)$ to be the image of $q(x)$ under the following linear transformation to remove the αxy term:

$$q'(x, y) = q(x + \frac{\alpha}{2}y, y) = x^2 - y^2\left(\frac{\alpha^2}{4} - 1\right) - k. \tag{6.19}$$

Now both $q'(x, y) = 0$ and $q(x, y) = 0$ have the same number of solutions in $\mathbb{F}_p^2$ since there is a bijection between their solutions. Now define $\Delta = \frac{\alpha^2}{4} - 1$. Below we present a theorem compiling the results in [4].

Theorem 6.3.1. *The number of solutions to* (6.17) *depends on the Legendre symbol* $\left(\frac{\Delta}{p}\right)$.

1. *For* $k \neq 0$
   - *if* $\left(\frac{\Delta}{p}\right) = 1$, *then there are* $p - 1$ *solutions to* $q'(x, y) = 0$.
   - *if* $\left(\frac{\Delta}{p}\right) = -1$, *then there are* $p + 1$ *solutions to* $q'(x, y) = 0$.

- *if* $\left(\frac{\Delta}{p}\right) = 0$, *then there are* $2p$ *solutions if* $\left(\frac{k}{p}\right) = 1$ *or no solutions if* $\left(\frac{k}{p}\right) = 0$.

2. *For* $k = 0$,

   - *if* $\left(\frac{\Delta}{p}\right) = 1$, *then there are* $2p - 1$ *solutions to* $q'(x, y) = 0$.
   - *if* $\left(\frac{\Delta}{p}\right) = -1$, *then there is* 1 *solution to* $q'(x, y) = 0$.
   - *if* $\left(\frac{\Delta}{p}\right) = 0$, *then there are* p *solutions to* $q'(x, y) = 0$.

See [4] for the proof which uses only elementary number theory. By considering all the level sets (i.e. all values of k) for a given p, for some fixed p and α we can classify the distribution of points on the p level sets.

Corollary 6.3.2. *The distribution of the* p^2 *points in* $\mathbb{F}_p^2$ *over the* p *level sets in* (6.17) *are as follows. We have three cases depending on the Legendre symbol* $\left(\frac{\Delta}{p}\right)$*:*

1. *If* $\left(\frac{\Delta}{p}\right) = 1$, *we have* $p - 1$ *level sets with* $p - 1$ *points each and one level set with* $2p - 1$ *points.*
2. *If* $\left(\frac{\Delta}{p}\right) = -1$, *we have* $p - 1$ *level sets with* $p + 1$ *points each and one level set with 1 point.*
3. *If* $\left(\frac{\Delta}{p}\right) = 0$, *there are* $\frac{p-1}{2}$ *level sets with* $2p$ *points each,* $\frac{p-1}{2}$ *level sets with* 0 *points each, and one level set with* p *points.*

This provides bounds on the possible lengths of the orbits. We now examine in more detail the possible orbit lengths (on each level set) of this linear mapping.

6.3.2 Orbit length and distribution

We will provide a more general result on the distribution of the periodic orbits for any mapping induced by a unimodular matrix. Let $A \in SL(2, \mathbb{Z})$, $A \neq \pm Id$. The result is stated in corollary 6.3.8. Let $\text{trace}(A) = \alpha$. Then A induces a toral automorphism on the 2-torus. We are interested in the periodic orbits on prime rational lattices with denominator p which is equivalent to solving the dynamics of (6.14) modulo p. We will show that all orbits have the same period which must be a divisor of $p - 1$ or $p + 1$. The lemma below provides a recursive identity for powers of A. This is obtained by repeatedly applying the Cayley-Hamilton theorem which says that A satisfies the matrix version of its characteristic polynomial.

Lemma 6.3.3. *We have the following recursive formula for $A \in SL(2,\mathbb{Z})$:*

$$A^k = u_k(\alpha)A - u_{k-1}(\alpha)Id, \tag{6.20}$$

where $u_k(\alpha)$ is a polynomial of degree $k-1$ in α such that

$$\begin{aligned} u_{k+2}(\alpha) &= \alpha u_{k+1}(\alpha) - u_k(\alpha), \qquad k \geq 0 \\ u_1(\alpha) &= 1 \\ u_0(\alpha) &= 0. \end{aligned} \tag{6.21}$$

(In the following, we will write u_k for $u_k(\alpha)$ for brevity.) Now since A has determinant 1, so does A^k and by using lemma 6.3.3 we have

$$\begin{aligned} \det(A^k) &= \det(u_k A - u_{k-1}Id) \\ &= u_k^2 \det(A) - u_k u_{k-1} \operatorname{trace}(A) + u_{k-1}^2 \\ &= u_k^2 - \alpha u_k u_{k-1} + u_{k-1}^2 \\ &= 1. \end{aligned} \tag{6.22}$$

Also,

$$\begin{aligned} \operatorname{trace}(A^k) &= u_k \operatorname{trace}(A) - 2u_{k-1} \\ &= \alpha u_k - 2u_{k-1}. \end{aligned} \tag{6.23}$$

Theorem 6.3.4. *Suppose that $\alpha \neq \pm 2$. The following are equivalent:*

1. $\operatorname{trace}(A^k) = 2 \pmod p$
2. $u_{k-1} = -1 \pmod p$ *and* $u_k = 0 \pmod p$
3. $A^k = Id \pmod p$.

Proof. (1) $\implies$ (2): Suppose $\alpha = 0$ and $\operatorname{trace}(A^k) = 2 \pmod p$. Then from (6.23)

$$\operatorname{trace}(A^k) = -2u_{k-1} = 2 \pmod p, \tag{6.24}$$

which gives us $u_{k-1} = -1$. Also, $u_k = 0 \pmod{p}$ because if $\alpha = 0$ every alternate term is 0. Now for $\alpha \neq 0$, suppose $\text{trace}(A^k) = 2 \pmod{p}$, then

$$\text{trace}(A^k) = \alpha u_k - 2u_{k-1} = 2 \pmod{p}. \tag{6.25}$$

Rearranging we get

$$\alpha u_k = 2(u_{k-1} + 1) \pmod{p} \tag{6.26}$$

and squaring,

$$u_k^2 = \frac{4}{\alpha^2}(u_{k-1} + 1)^2 \pmod{p}. \tag{6.27}$$

Now substituting (6.26) and (6.27) into (6.22) to eliminate u_k and simplifying we get

$$(4 - \alpha^2)(u_{k-1} + 1)^2 = 0 \pmod{p} \tag{6.28}$$

which gives us the solution $u_{k-1} = -1 \pmod{p}$ and $u_k = 0 \pmod{p}$ $(\alpha \neq 0)$.

(2) $\implies$ (3): Suppose $u_{k-1} = -1 \pmod{p}$ and $u_k = 0 \pmod{p}$. Then substituting into (6.20) we get

$$A^k = Id \pmod{p}. \tag{6.29}$$

(3) $\implies$ (1): Suppose $A^k = Id \pmod{p}$. Then it is clear $\text{trace}(A^k) = 2 \pmod{p}$. □

Corollary 6.3.5. *If $\alpha \neq \pm 2$ all orbits of the dynamical system induced by A modulo p have the same period length t.*

Proof. Suppose z is periodic with (minimum) period length k. Then we have

$$A^k z = z \pmod{p}. \tag{6.30}$$

Rearranging,

$$(A^k - Id)z = \mathbf{0} \pmod{p}. \tag{6.31}$$

For non-trivial solutions we must have

$$\det(A^k - Id) = \det(A^k) + 1 - tr(A^k) = 0 \pmod{p}. \tag{6.32}$$

Now A is unimodular so $\det(A^k) = 1$. Thus we have $\text{trace}(A^k) = 2 \pmod p$. But by theorem 6.3.4, we get

$$A^k = Id \pmod p. \tag{6.33}$$

This tells us that all points must have period a divisor of k. Now suppose z' is periodic with minimum period length d where $d \mid k$. Following the same argument, we get that

$$A^d = Id \pmod p. \tag{6.34}$$

But this also shows that

$$A^d z = z \pmod p. \tag{6.35}$$

Since k was chosen to be the (minimum) period length of z we get that $d = k$. Thus, if z has minimum period k, z' must also have minimum period k. □

Here we see that $\text{trace}(A^k) = 2 \pmod p$ is a necessary and sufficient condition for period k cycles. (Note k here is not necessarily the minimal period.) We will now show how to find possible values of k for a given A. The binary recurrence sequence (6.21) is a Lucas sequence [42]. For $\alpha \neq \pm 2$, this recurrence relation has solution given by

$$u_n = \frac{\beta^n - \gamma^n}{\beta - \gamma}, \tag{6.36}$$

where

$$\beta = \frac{\alpha + \sqrt{\alpha^2 - 4}}{2}, \qquad \gamma = \frac{\alpha - \sqrt{\alpha^2 - 4}}{2}. \tag{6.37}$$

It is useful to note that

$$\beta + \gamma = \alpha, \qquad \beta - \gamma = \sqrt{\alpha^2 - 4}, \qquad \beta\gamma = 1. \tag{6.38}$$

Now we let $\Delta = (\beta - \gamma)^2 = \alpha^2 - 4$. Then we have the following theorem (Theorem 2.2.4 in [42]). This theorem provides a specific k for which $\text{trace}(A^k) = 2 \pmod p$ from theorem 6.3.4 for $\alpha \neq \pm 2$.

Theorem 6.3.6. *Let p be a prime number. We have the following properties:*

1. *If $(\Delta/p) = 1$, then $u_{p-1} = 0 \pmod p$ and $u_{p-2} = -1 \pmod p$.*
2. *If $(\Delta/p) = -1$, then $u_{p+1} = 0 \pmod p$ and $u_p = -1 \pmod p$.*

Proof. **1.:** Suppose $(\Delta/p) = 1$. Let us consider β^p:

$$\beta^p = \left(\frac{\alpha + \sqrt{\Delta}}{2}\right)^p \tag{6.39}$$

$$= \frac{1}{2^p}\left(\alpha^p + \Delta^{p/2} + \sum_{k=1}^{p-1}\binom{p}{k}\alpha^{p-k}\Delta^{k/2}\right) \tag{6.40}$$

$$= \frac{1}{2^p}(\alpha^p + \Delta^{p/2}) \pmod{p}. \tag{6.41}$$

Now rearrange to get

$$2^p\beta^p = \alpha^p + \Delta^{(p-1)/2}\sqrt{\Delta} \pmod{p} \tag{6.42}$$

$$= \alpha^p + \sqrt{\Delta} \pmod{p}, \tag{6.43}$$

where we have used that $(\Delta/p) = 1$. Now p is an odd prime, so $2^p = 2 \pmod{p}$ and $\alpha^p = \alpha \pmod{p}$ (Fermat's little theorem). This gives us

$$2\beta^p = \alpha + \sqrt{\Delta} = 2\beta \pmod{p}. \tag{6.44}$$

So finally we obtain $\beta^p = \beta \pmod{p}$ and $\beta^{p+1} = \beta^2 \pmod{p}$. The same congruences are obtained if we change β to γ, that is, $\gamma^p = \gamma \pmod{p}$ and $\gamma^{p+1} = \gamma^2 \pmod{p}$. Subtracting these congruences we get

$$(\beta - \gamma)(u_p - 1) = 0 \pmod{p} \qquad \text{and} \qquad (\beta - \gamma)(u_{p+1} - \alpha) = 0 \pmod{p}. \tag{6.45}$$

From this we obtain $p \mid \sqrt{\Delta}(u_p - 1)$ and $p \mid \sqrt{\Delta}(u_{p+1} - \alpha)$ but $p \nmid \Delta$, so $u_p = 1 \pmod{p}$ and $u_{p+1} = \alpha \pmod{p}$. Now using the recurrence (6.21) and reducing modulo p with $k = p - 1$,

$$u_{p+1} = \alpha u_p - u_{p-1} \pmod{p} \tag{6.46}$$

gives us

$$\alpha = \alpha - u_{p-1} \pmod{p}, \tag{6.47}$$

and so we get $u_{p-1} = 0 \pmod{p}$. Applying the recurrence again with $k = p-2$ we obtain $u_{p-2} = -1 \pmod{p}$ as required.

(2): We use the same technique as (1) but now with $(\Delta/p) = -1$.Suppose $(\Delta/p) = -1$. Then

$$2\beta^p = \alpha - \sqrt{\Delta} = 2\gamma \pmod{p}. \tag{6.48}$$

This gives us the equations

$$\beta^p = \gamma \pmod{p}, \qquad \text{and} \qquad \beta^{p+1} = \beta\gamma = 1 \pmod{p}. \tag{6.49}$$

The same argument also gives us

$$\gamma^p = \beta \pmod{p}, \qquad \text{and} \qquad \gamma^{p+1} = \beta\gamma = 1 \pmod{p}, \tag{6.50}$$

and subtracting these equations we get

$$\sqrt{\Delta}(u_p + 1) = 0, \qquad \text{and} \qquad \sqrt{\Delta}u_{p+1} = 0 \pmod{p}, \tag{6.51}$$

from which we obtain $u_p = -1 \pmod{p}$ and $u_{p+1} = 0 \pmod{p}$ as required. □

We now present the main result of this subsection. This was first obtained by Percival and Vivaldi [55] for general linear maps using ideal theory but our proof and methods are completely different. Here we present a new proof of this for our linear system using elementary number theory.

Theorem 6.3.7. *Let* $\Delta = \alpha^2 - 4$.

1. *If* $(\Delta/p) = -1$ *then* $A^{p+1} = Id \pmod{p}$.
2. *If* $(\Delta/p) = 1$ *then* $A^{p-1} = Id \pmod{p}$.
3. *If* $(\Delta/p) = 0$ *we have two cases:*

   i) for $\alpha = 2 \pmod{p}$ *we have* $A^p = Id \pmod{p}$.

   ii) for $\alpha = -2 \pmod{p}$ *we have* $A^p = -Id \pmod{p}$.

Proof. (1) and (2) follow directly from theorem 6.3.6 and theorem 6.3.4.

(3i): Consider the case when $(\Delta/p) = 0$ where $\alpha = 2 \pmod p$. Then, it is easy to show that the solution to the recurrence (6.21) is $u_k = k \pmod p$. In particular, $u_p = 0 \pmod p, u_{p-1} = -1 \pmod p$. Then putting $k = p$ in (6.20) and reducing modulo p

$$A^p = Id \pmod p \tag{6.52}$$

as required.

(3ii): Now we consider $(\Delta/p) = 0$ where $\alpha = -2 \pmod p$. Here the solution to the recurrence (6.21) is $u_k = (-1)^{k+1}k \pmod p$. In particular $u_p = 0 \pmod p$ and $u_{p-1} = 1 \pmod p$ (since p is odd). Then putting $k = p$ in (6.20) and reducing modulo p

$$A^p = -Id \pmod p \tag{6.53}$$

as required. □

Corollary 6.3.8. *From theorem 6.3.4 and 6.3.7 it follows that:*

1. *If $(\Delta/p) = -1$ then all orbits have the same period t which is a divisor of $p+1$. If $t = (p+1)/m$, then there are $m(p-1)$ orbits.*
2. *If $(\Delta/p) = 1$ all orbits have the same period t which is a divisor of $p-1$. If $t = (p-1)/m$, then there are $m(p+1)$ orbits.*
3. *If $(\Delta/p) = 0$ we have two cases:*
   - *i) for $\alpha = 2 \pmod p$ there are $p-1$ fixed points and $p-1$ orbits of period p.*
   - *ii) for $\alpha = -2 \pmod p$ there are $(p-1)/2$ orbits of period 2 and $(p-1)/2$ orbits of period $2p$.*

Proof. Cases (1) and (2) follow directly as corollary 6.3.5 showed that for $\alpha \neq \pm 2$ all orbits have the same period, and theorem 6.3.7 showed that they must divide $p+1$ or $p-1$ respectively. Now theorem 6.3.4 does not apply for case (3). For (3i), we have that $A^p = Id \pmod p$ from theorem 6.3.7. This tells us that all orbits must be a divisor of p. But the only divisors of p are 1 and itself. Now for $\text{trace}(A) = 2$ and for $A \neq Id$ we will get $p-1$ fixed points (note we don't include the origin). Then the rest of the space must be consumed in cycles of length p and the result follows.

(3ii): In this case we have $A^p = -Id \pmod p$ from which we obtain $A^{2p} = Id \pmod p$. This tells us that all orbits must be a divisor of $2p$ which has divisors $1, 2, p, 2p$. Now $\text{trace}(A) = -2$ and $\text{trace}(A^p) = -2$ so we cannot get any fixed points or period p orbits. Now if $A^2 \neq Id \pmod p$ then we will get $(p-1)/2$ orbits of period 2 (eigenspace has $p-1$ points excluding origin). The rest of the phase space must be consumed in period $2p$ orbits and the result follows. □

This describes the distribution of orbits on $\mathbb{F}_p^2$. Thus our period distribution will be a singular distribution as all orbits have the same period. Notice that corollary 6.3.8 is consistent with corollary 6.3.2. In table 6.1 we show this result for $\alpha = 5$ with the map in (6.14) and for various primes. Note that origin $(0, 0)$ is excluded as it is a fixed point.

Table 6.1: Period length and number of orbits of f_α in (6.14) with parameter $\alpha = 5$.

p	(Δ/p)	# orbits	period length.
11	-1	10	12
13	-1	12	14
17	1	18	16
19	-1	36	10
23	-1	66	8
29	-1	168	5
31	-1	60	16
37	1	152	9

Now for a fixed prime p we may be interested in the distribution of the scaled period t/p for each parameter $\alpha \neq \pm 2 \pmod p$. From corollary 6.3.8 we know that t is a divisor of $p+1$ or $p-1$. Figure 6.4 displays this distribution. The distribution has been studied for the generalised Cat maps and Chen et al. [13] give the explicit number of parameter values for which we see each period. By applying their results, we can obtain a similar one for our one parameter cat map in (6.14) which follows.

Theorem 6.3.9. *For each $t > 2$ and $t|p \pm 1$ there are $\frac{\phi(t)}{2}$ parameter values corresponding to common period t where $\phi(t)$ is the Euler totient function, the number of positive integers up to t that are coprime to t.*

Example 6.3.10. Table 6.2 displays the results that we see for $p = 769$ where the first column t shows the periods we see, the second column $\#\alpha$ shows the number of parameter values α where t was the minimum period of the orbits, and the third column is the value $\phi(t)/2$.

Table 6.2: Table of the period t and number of parameter values. Left for $t|p+1$, right for $t|p-1$ for $p = 769$. Note that $770 = 2.5.7.11$ and $768 = 2^8.3$.

t	$\#\alpha$	$\phi(t)/2$
5	2	2
7	3	3
10	2	2
11	5	5
14	3	3
22	5	5
35	12	12
55	20	20
70	12	12
77	30	30
110	20	20
154	30	30
385	120	120
770	120	120
sum	384	384

t	$\#\alpha$	$\phi(t)/2$
3	1	1
4	1	1
6	1	1
8	2	2
12	2	2
16	4	4
24	4	4
32	8	8
48	8	8
64	16	16
96	16	16
128	32	32
192	32	32
256	64	64
384	64	64
768	128	128
sum	383	383

As we vary α and $\alpha \neq \pm 2 \pmod{p}$, we have a total of $p-2$ cat maps. From the table we see that $384 + 383 = 767$ where we have not included parameters $a = \pm 2 \pmod{p}$ since not all orbits have the same period. In fact, it is well known from number theory that

$$\sum_{i|N} \phi(i) = N, \tag{6.54}$$

so performing the summation for divisors of $N+1$ and $N-1$ which are greater than 2,

$$\sum_{i>2, i|p+1} \frac{\phi(i)}{2} + \sum_{i>2, i|p-1} \frac{\phi(i)}{2} = \frac{p+1-\phi(2)-\phi(1)}{2} + \frac{p-1-\phi(2)-\phi(1)}{2} = p-2 \tag{6.55}$$

Remark 6.3.11. For $\alpha = -1, 0, 1 \pmod{p}$ the matrix A_α (6.13) is conjugate to the rotation matrix with angle of rotation given by $\theta = \pi/3, \pi/4, \pi/6$ respectively and so have all orbits with period $3, 4$ and 6 respectively. This is consistent with corollary 6.3.8. For example, consider $\alpha = 0$. So $\Delta = -4$. Then the Legendre symbol is

$$\left(\frac{\Delta}{p}\right) = \left(\frac{-4}{p}\right) = \left(\frac{4}{p}\right)\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}} = \begin{cases} 1 & \text{if } p = 1 \pmod 4 \\ -1 & \text{if } p = 3 \pmod 4. \end{cases} \tag{6.56}$$

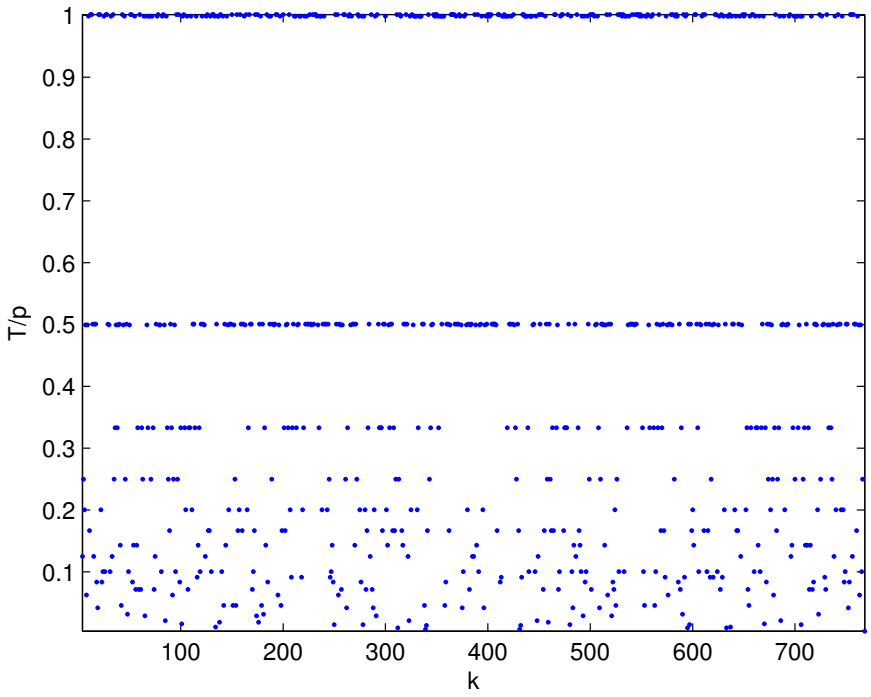


Figure 6.3: Plot of the scaled period t/p of orbits of f_α (6.14) for $\alpha \neq \pm 2 \pmod{p}$ for $p = 769$. Note that there are values at $\frac{p+1}{p}, \frac{p-1}{p}$ and for $\frac{p+1}{2p}, \frac{p-1}{2p}$ and so on which may be hard to distinguish in the plot.

So if $p = 4n + 1$, then the theorem tells us that all orbits have the same period which is a divisor of $p - 1 = 4n$. Alternatively, if $p = 4n + 3$, the theorem tells us that all orbits have the period which is a divisor of $p + 1 = 4n + 4$. In both cases this is consistent as we know for $k = 0$ all orbits have period 4. Similar analysis can be done for $k = \pm 1$.

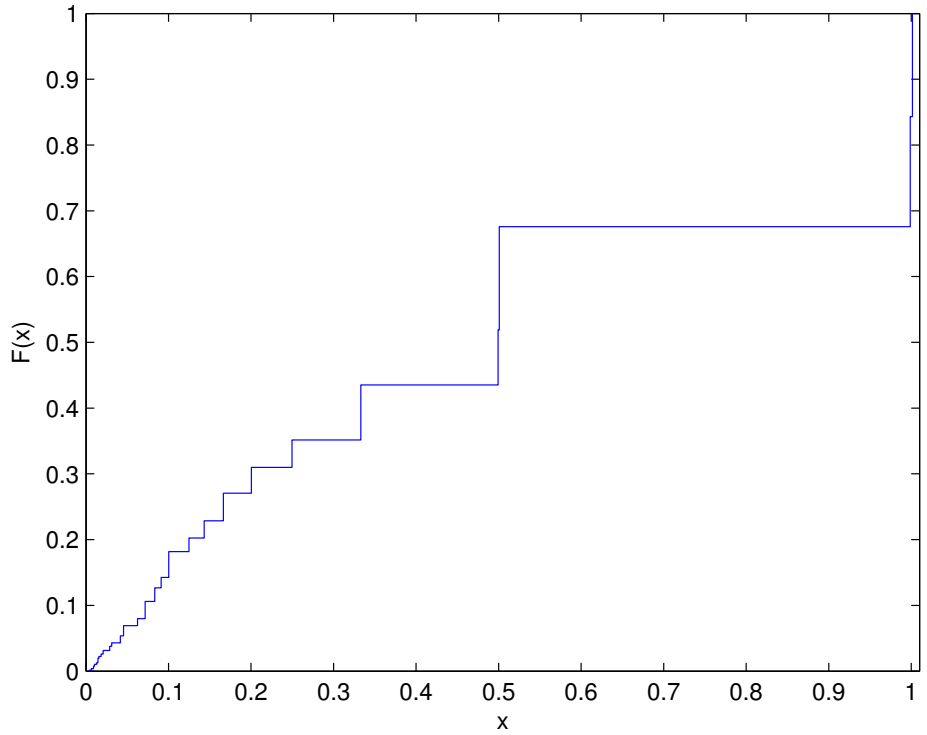


Figure 6.4: Plot of the cumulative distribution function for the scaled periods, i.e. the proportion $F(x)$ of parameters $\alpha \neq \pm 2 \pmod{p}$ for f_α (6.14) where $t/p \leq x$.

6.4 Nonlinear map with integral in 2D

In the previous section we considered the dynamics of a family of linear maps over the finite field, showing the effect of an integral of motion. We saw that conic sections have tight bounds on the number of points in the finite field. For nonlinear maps, their integrals typically will be of higher degree (genus). We also want to know how the number of points are distributed among the level sets of the integral. This problem was solved by Hasse for elliptic curves and later in general by Weil. The Hasse-Weil Bound provides the bounds for this number, and for irreducible algebraic curves on the number of points N on the curve C of genus $g \geq 1$ over the finite field $\mathbb{F}_p$ is bounded by

$$|N - (p+1)| \leq 2g\sqrt{p}. \tag{6.57}$$

Roberts et al. [61] showed that this bound was effective as a test for integrability (and distinguishing near-integrability) for a family of (reversible) maps, as any particular orbit cannot exceed the upper bound $p + 1 + 2g\sqrt{p}$. This was used to develop a Monte-Carlo type test for integrability by computing the length of orbit of a point for various primes p, and if the length of any was outside the Hasse-Weil bound, either the integral was

reducible or the map did not have an integral. It will be useful to have a running example of a two dimensional map with one integral. Consider over the finite space $\mathbb{F}_p^2$ the three parameter family (ϵ, ξ, λ) of QRT maps which are reversible given by

$$x' = -x - \frac{\epsilon y + \xi}{y^2 + 1}, \qquad y' = -y - \frac{\epsilon x' + \lambda}{(x')^2 + 1}, \tag{6.58}$$

which has integral

$$I(x, y) = x^2 y^2 + x^2 + y^2 + \epsilon xy + \xi x + \lambda y. \tag{6.59}$$

This is an elliptic curve of genus 1. The QRT map has reversing symmetries H, G

$$H : x' = x,\ y' = -y - \frac{\epsilon x + \lambda}{x^2 + 1}, \qquad G : x' = -x - \frac{\epsilon y + \xi}{y^2 + 1},\ y' = y. \tag{6.60}$$

We will consider the orbit statistics for this map across various primes p and parameter values. For $p = 3 \pmod 4$, the map is a permutation as the denominator is non-zero and all orbits are periodic. For $p = 1 \pmod 4$, there will be singularities and thus singular (terminating) orbits.

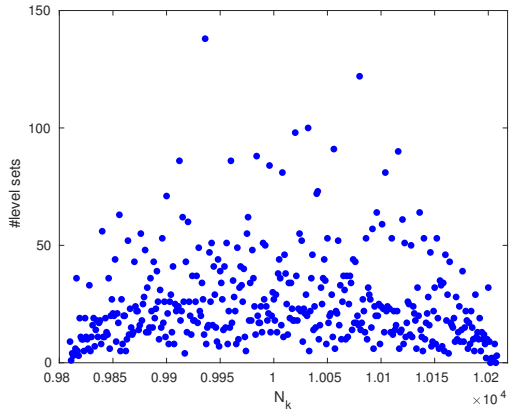
This family of QRT maps was used as an example to show the efficacy of the orbit length test for integrability. It should be noted that in many instances, the orbit length of a point was near the upper bound, when the level set consisted of just one (symmetric) orbit. Of interest is also the distribution of the number of points on level sets. We plot this in figure 6.5a. The problem of the distribution of the number of points on elliptic curves over finite fields has been of interest in number theory. For a fixed prime p, let N_k be the number of points on the level set with value k, that is where $I(x, y) = k$, for $k = 0, \ldots, p-1$. Then with each k by using (6.57) with $g = 1$ we can associate a θ_k where

$$p + 1 - N_k = 2\sqrt{p}\cos\theta_k, \qquad (0 \le \theta_k \le \pi). \tag{6.61}$$

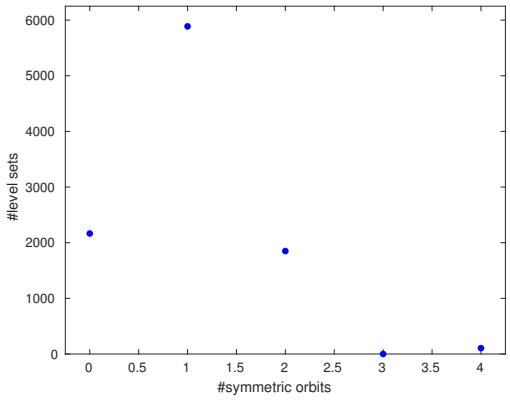
For a fixed elliptic curve and increasing p, the Sato-Tate [73] conjecture states that for $0 \le a < b \le \pi$, the density of the set of primes p (in the limit) for which $a \le \theta_k \le b$, exists and is equal to

$$\frac{2}{\pi}\int_a^b \sin^2\theta d\theta = \frac{1}{\pi}\left[\theta - \frac{\sin(2\theta)}{2}\right]_a^b. \tag{6.62}$$

This was first proved by Taylor [74] under mild conditions and he and others have made improvements in some papers following [see [15][28]]. However, here we are interested in



(a) Histogram of number of points on level sets for QRT map showing that they are within the Hasse-Weil bounds of 9808 and 10208 as the minimum and maximum value is 9810 and 10208 respectively.



(b) Histogram of number of symmetric orbits on each level set. There are $2165, 5887, 1850, 0, 105$ level sets with $0, 1, 2, 3, 4$ symmetric orbits respectively.

Figure 6.5: Both figures are for the QRT map with $p = 10007$ and parameters $(\epsilon, \xi, \lambda) = (8, 25, 13)$

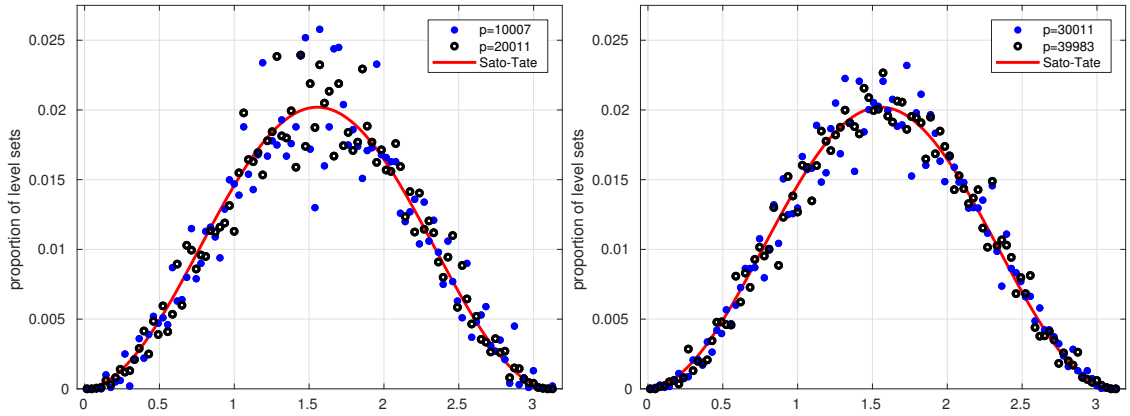
Table 6.3: The 1-norm distance of partitions from Sato-Tate

p	1-norm
10007	0.1400
20011	0.1056
30011	0.0904
39983	0.0735

the distribution of the points for fixed p and varying elliptic curves over a one-parameter family. This was studied by Birch in 1968 [7] showing that we expect to have a distribution that approximates the Sato-Tate conjecture (6.62) when p is large. We can look at the distribution of θ_k by doing a histogram of 99 equal partitions of $[0, \pi]$. We plot this in figure 6.6 for $p = 10007, 20011, 30011, 39983$ where the value of the red curve is given by (6.62) for each partition. We can calculate the distance of our experimental data from this using the 1-norm which is shown in table 6.3.

Furthermore, Jogia et al. [33] showed that the action of birational maps in two dimensions with an integral is conjugate to addition on a Weierstrass cubic.

Theorem 6.4.1. *([33] Theorem 4) Let L be an infinite order birational map defined over $\mathbb{C}(t)$ that preserves an algebraic foliation $C(x, y, t) = 0$ where $C = E/\mathbb{C}(t)$ is an elliptic curve. Then L is conjugate to a map $\tilde{L} : P \mapsto P + \Omega(t)$ on the associated Weierstrass $W/\mathbb{C}(t)$, where $\Omega(t) = (\omega_1(t), \omega_2(t))$ and $\omega_i(t) \in \mathbb{C}(t)$. Furthermore, L is reversible, i.e., can be written as the composition of two rational involutions over $\mathbb{C}(t)$, and the dynamics of L on each curve can be parametrized in terms of Weierstrass elliptic functions.*



(a) Histogram of θ_k in 99 equal partitions of $[0, \pi]$ with $p = 10007$ and $p = 20011$.

(b) Histogram of θ_k in 99 equal partitions of $[0, \pi]$ with $p = 30011$ and $p = 39983$.

Figure 6.6: Plots of θ_k for large p.

This means that for the QRT map all (periodic) orbits on each level set have the same period. This is similar to the result for the linear map in the previous section. For each level set with value $k = I(x, y)$, let α_k be the common period and β_k be the number of orbits of length α_k. Then using the Hasse-Weil bound (6.57) we get in the case $p = 3 \pmod 4$ where the QRT map is a permutation

$$p + 1 - 2\sqrt{p} \leq \beta_k \alpha_k \leq p + 1 + 2\sqrt{p}. \tag{6.63}$$

Then for fixed p and arbitrary k, since $\beta \in \mathbb{Z}^+$ we obtain the possible periods of α_k

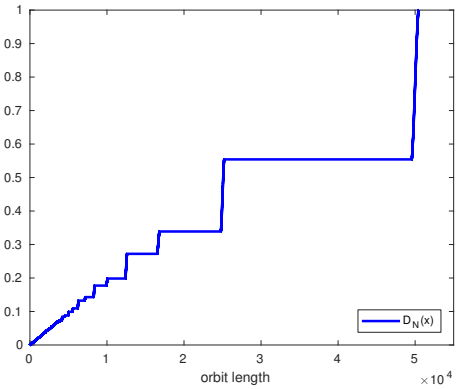
$$\frac{1}{n}(p + 1 - 2\sqrt{p}) \leq \alpha_k \leq \frac{1}{n}(p + 1 + 2\sqrt{p}), \qquad n = 1, 2, \ldots \tag{6.64}$$

This gives us a series of allowed intervals for α_k. The Hasse-Weil Bound (6.57) tells us that the number of points on a level set must lie in the interval $[p+1-2\sqrt{p}, p+1+2\sqrt{p}]$. Thus, the allowable periods lie in the intervals

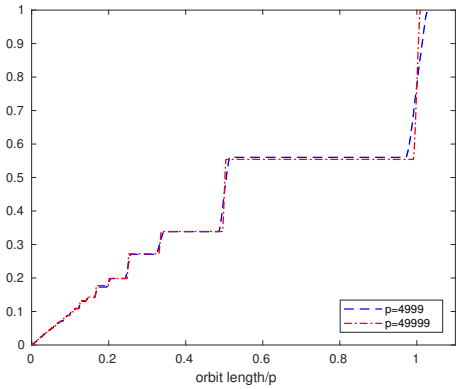
$$\rho_n(p) := \left[\frac{1}{n}(p + 1 - 2\sqrt{p}), \frac{1}{n}(p + 1 + 2\sqrt{p})\right], \qquad n = 1, 2, \ldots. \tag{6.65}$$

With p fixed, for large enough n, these intervals will overlap. This occurs when the upper bound of $p_{n+1}(p)$ is greater than or equal to the lower bound of $p_n(p)$, that is,

$$\frac{1}{n+1}(p + 1 + 2\sqrt{p}) \geq \frac{1}{n}(p + 1 - 2\sqrt{p}), \tag{6.66}$$



(a) QRT: Cumulative distribution of orbits for $p = 49999$ with $\epsilon = 3, \lambda = 5, \xi = 2$.



(b) QRT: Cumulative distribution of orbits for $p = 4999$ and $p = 49999$ showing similar heights for the step sizes.

Figure 6.7

which gives

$$n \geq \frac{\sqrt{p}}{4} + \frac{1}{4\sqrt{p}} - \frac{1}{2}, \tag{6.67}$$

and we define

$$n_p := \left\lceil \frac{\sqrt{p}}{4} + \frac{1}{4\sqrt{p}} - \frac{1}{2} \right\rceil, \tag{6.68}$$

the smallest integer such that the intervals overlap. Thus this gives restrictions on the possible orbit lengths for large period lengths. This can be seen in the plateaus (which signify there are no orbits of such lengths) in figure 6.7 (note these p values satisfy $p = 3 \pmod 4$).

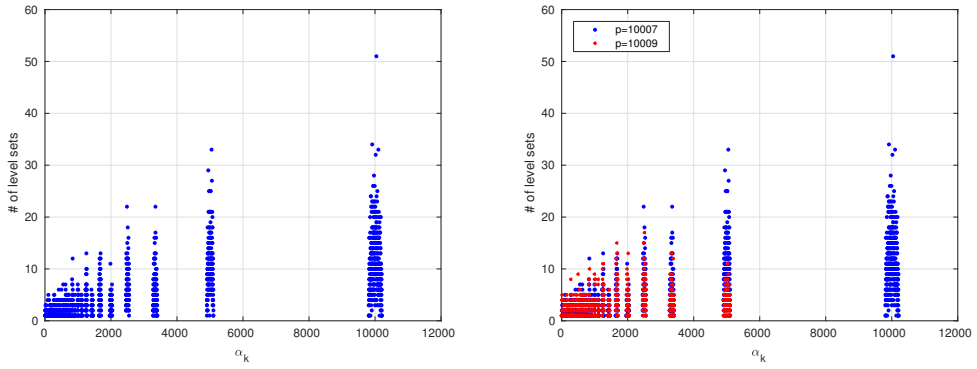
Example 6.4.2. Consider the QRT map (6.58) with $p = 4999$ and $\epsilon = 3, \lambda = 5, \xi = 2$. The first few intervals of allowable periods (rounding to integers) are

$$\rho_1 = [4859, 5141], \rho_2 = [2430, 2570], \rho_3 = [1620, 1713], \rho_4 = [1215, 1285], ... \tag{6.69}$$

Thus, there can be no periods from 2571 to 4858, 1714 to 2429 and so on. Furthermore, we have $n_p = 18$ and $\rho_{18} = [270, 285]$, and thus $\cup_{i=18}^{\infty} \rho_i = [1, 285]$ and all periods from 1 to 285 are possible.

6.5 The number of symmetric and asymmetric periodic orbits in the QRT map

In this section we consider the number of cycles in the QRT map over $\mathbb{F}_p^2$. We compare this number with other maps considered previously also over $\mathbb{F}_p^2$. Recall from chapter 3 that the expected number of cycles for a polynomial automorphism over $\mathbb{F}_p^2$ is H_{p^2} of



(a) Histogram of period α_k for the QRT map (6.58) for $p = 10007$ with parameters (8,25,13).

(b) Histogram of α_k for the QRT map (6.58) for $p = 10007$ (blue) and $p = 10009$ (red) with parameters (8,25,13).

Figure 6.8: These figures show the effect of singularities on the distribution of α_k for the QRT map (6.58). We see that the larger values of α_k disappear for $p = 10009$ while the smaller α_k remain the same.

(3.3), and from chapter 4 that the expected number of cycles for a birational map over $\mathbb{F}_p^2$ is $H_{p^2} - H_s$ where H_n is the nth harmonic number and s is the number of singular points of the map. Recall from chapter 5, the number of symmetric cycles for reversible polynomial automorphisms is $\frac{1}{2}\#\text{Fix}(G) + \#\text{Fix}(H))$ (see corollary 5.3.1), and that the number of cycles is close to this lower bound in general. The QRT is also reversible, so we can also further divide the cycles into symmetric or asymmetric.

6.5.1 QRT map with no singularities

For the QRT map (6.58) with no singularities, the number of symmetric periodic orbits can be calculated from the fixed sets of G and H using corollary 5.3.1. Since the cardinalities of $\text{Fix}(G)$ and $\text{Fix}(H)$ are both p from (6.60), then we have

$$\#\text{symmetric cycles} = \frac{p+p}{2} = p. \tag{6.70}$$

Recall that theorem 6.4.1 tells us all periodic orbits on the same level set have the same orbit length. Then we need to know the distribution of these periods for each level set. A figure of this is shown for $p = 10007$ and $p = 10009$ in figure 6.8. Without any better way to proceed, we assume that these follow a uniform distribution. This is not accurate since as mentioned before, there are windows of disallowable periods. However, we see that this is a good approximation as level sets with large α_k in (6.63) contribute relatively little to the number of (symmetric) periodic orbits. Most of the contribution will be with small

α_k meaning there will be many periodic orbits on the corresponding level set. Using this idea, we consider the number of cycles. This is given by the sum of β_k (see (6.63)). So we have

$$\begin{aligned}
\#\text{cycles} &= \sum_{k=0}^{p-1} \beta_k \\
&\approx \sum_{k=0}^{p-1} \frac{p}{\alpha_k} \qquad \text{(using the Hasse-Weil bound)} \\
&\approx p \sum_{k=1}^{p} \frac{1}{k} \qquad \text{(assuming uniform distribution of } \alpha_k\text{)} \\
&= pH_p.
\end{aligned} \tag{6.71}$$

There are few things to notice here. Recall from section 3.2.1 that the expected number of cycles for the dissipative Hénon map was H_{p^2}. This is essentially a magnitude of p times more. In fact, it is p times the expected number of cycles in a random permutation with p points. This is similar to the expected number of cycles for the 3D dissipative Hénon map with 1 integral in (6.5). We will see these ideas again in the later chapters how each additional integral multiplies the number of (asymmetric) cycles by a factor of p. Then it follows from (6.70) and (6.71) that we have

$$\#\text{asymmetric cycles} = \#\text{cycles} - \#\text{symmetric cycles} \tag{6.72}$$

$$\approx pH_p - p \tag{6.73}$$

$$= p(H_p - 1). \tag{6.74}$$

Again, we note that the number of (asymmetric) cycles is an approximation but the important part is the leading term behaviour which is vastly different to the other types of maps for example the expected number of cycles in a random permutation. The accuracy of this model is shown in figure 6.9.

6.5.2 QRT map with singularities

For the QRT map (6.58) with singularities, we need to consider the effect of singularities as they will consume a proportion of the space in singular orbits. From numerical experiments, it seems that for the QRT map with singular points, that we have

$$\#\text{symmetric cycles} \approx \frac{2p}{7}, \tag{6.75}$$

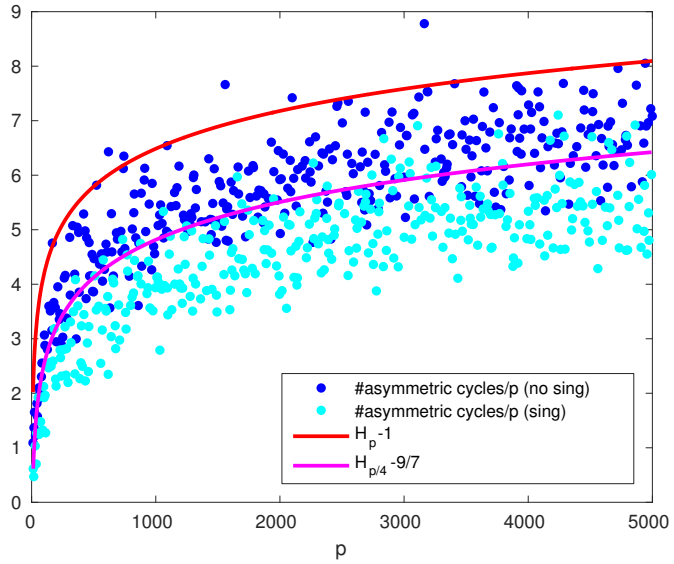


Figure 6.9: The number of asymmetric cycles divided by prime p in the QRT map (6.58) for parameters $(\epsilon, \xi, \lambda) = (3, 2, 5)$ compared to a heuristic model.

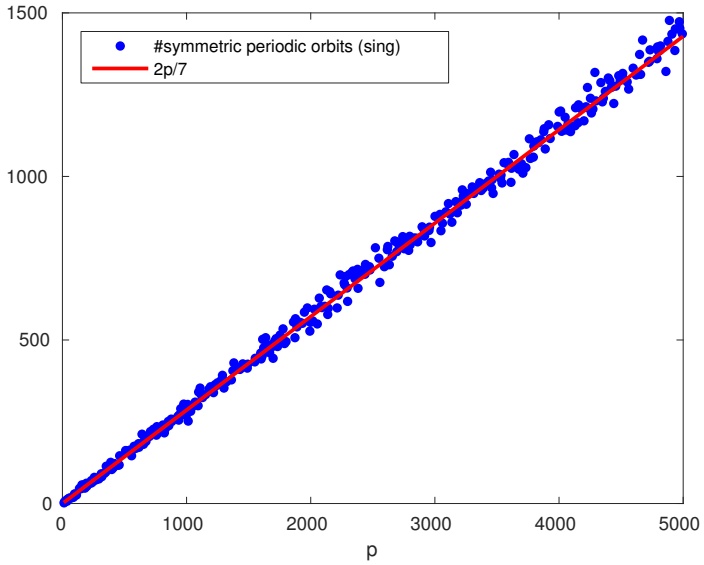


Figure 6.10: The number of symmetric periodic orbits in the QRT map (6.58) for parameters $(\epsilon, \xi, \lambda) = (3, 2, 5)$ for $p = 1 \pmod 4$ compared with $\frac{2p}{7}$. Note that for $p = 3 \pmod 4$ the number is exactly p.

as shown in figure 6.10.

Now we want to find the total number of cycles. We use a basic model to consider the effect of the singular points in reducing the number of cycles on each level set. From (6.58) there are $4p$ singular points when $p = 1 \pmod 4$ since -1 is a quadratic residue and almost all the level sets have exactly four singular points. Experimentally, we generally obtain four asymmetric singular orbits of the same length as the periodic orbits (we may also see pairs of asymmetric singular orbits which combine to be of that same length).

Thus, when comparing with the case of no singularities, we can subtract four cycles for each level set with four or more cycles. Figure 6.8 shows the loss of long periodic orbits for $p = 10009$ (singularities) when compared $p = 10007$ (no singularities). So to account for this, we count the number of cycles β_k of period α_k for level sets with greater than four cycles. That is,

$$\begin{aligned}
\#\text{cycles} &\approx \sum_{k=0}^{p-1} \max(\beta_k - 4, 0) && (6.76)\\
&\approx \sum_{k=0}^{p-1} \max\left(\frac{p}{\alpha_k} - 4, 0\right) && (6.77)\\
&\approx \sum_{k=1}^{p} \max\left(\frac{p}{k} - 4, 0\right) \qquad \text{(assuming equidistribution of } \alpha_k\text{)} && (6.78)\\
&= p \sum_{k=1}^{\lfloor p/4 \rfloor} \frac{1}{k} - p && (6.79)\\
&\approx pH_{p/4} - p. && (6.80)
\end{aligned}$$

Thus, we have that

$$\begin{aligned}
\#\text{asymmetric cycles} &= \#\text{cycles} - \#\text{symmetric cycles} && (6.81)\\
&\approx (pH_{p/4} - p) - 2p/7 && (6.82)\\
&= p(H_{p/4} - 9/7). && (6.83)
\end{aligned}$$

In figure 6.9 we compare the number of asymmetric cycles divided by p with the heuristic model. We see that it is a good approximate fit, albeit generally overestimating. However, when we consider the expected statistics of H_{p^2} and at least p for the dissipative Hénon map and the area-preserving reversible Hénon map respectively, we can see a vast difference in the number of cycles which is shown in figure 1.1. This gives some preliminary evidence that the number of cycles in the finite field can be a good discriminator of the algebraic properties of integrability and reversibility.

6.6 Basic model for number of asymmetric periodic orbits for with integrals

In this section, we generalise the ideas above to count the number of asymmetric periodic orbits for any reversible map that has the same cycle lengths on level sets. This will be a heuristic argument using similar assumptions to the model for the QRT map. In

particular, we assume that there is equidistribution of the cycle lengths on level sets. We also assume uniformity in how the symmetric and singular points are distributed and their effect on cycle lengths. It is necessary to do this because there is not much that has been proved regarding these and it seems to be difficult to have any meaningful results in generality.

Suppose L is a d-dimensional map with j integrals. Let $N = p^d$ be the number of points in our space. We will use the following notation throughout the rest of the thesis. We let g denote $\#\mathrm{Fix}(G)$, the cardinality of the fixed set of G, and similarly h denote $\#\mathrm{Fix}(H)$, the cardinality of the fixed set of H. We also let γ, η denote the singular set of G and H respectively. Then the number of fixed points of the involutions is $g + h$ and the number of singular points be $\gamma + \eta$. Each j-tuple of heights of each integral represent a different intersection of level sets. Suppose there are p^j level sets with the number of points distributed uniformly, so each level set has

$$\frac{N}{p^j} \tag{6.84}$$

points,

$$\frac{g+h}{p^j} \tag{6.85}$$

fixed points of involutions and

$$\frac{\gamma+\eta}{p^j} \tag{6.86}$$

singular points. Now any orbit without any fixed points of G or H or singular points will be an asymmetric cycle. We will model this number. For each level set, we will simply subtract the number of possible symmetric cycles and the number of singular orbits and consider over all level sets. Now let α_m and β_m denote respectively the common length of the cycles and the number of cycles on the mth level set, $1 \leq m \leq p^j$. Consider the number of asymmetric cycles of length k. We define a k-level set as a level set with $\alpha_m = k$. On a k-level set with no singularities, the number β_m of k-periodic cycles is on

average $N/(kp^j)$. Then,

$$\#\text{asymmetric } k\text{-cycles} = \#k\text{-level set.} \left(\frac{N}{kp^j} - \frac{g+h}{2p^j} - \frac{\gamma+\eta}{p^j} \right) \tag{6.87}$$

$$= \frac{p^{2j}}{N} \left(\frac{N}{kp^j} - \frac{g+h}{2p^j} - \frac{\gamma+\eta}{p^j} \right) \tag{6.88}$$

$$= p^j \left(\frac{1}{k} - \frac{g/2+h/2+\gamma+\eta}{N} \right) \tag{6.89}$$

where we have used that $\#k\text{-level set} = p^{2j}/N$. This is because there are p^j level sets with possible values of α_m from 1 to approximately N/p^j, and by assuming a uniform distribution, we get $\#k\text{-level set} = \#\{\alpha_m \mid \alpha_m = k\} = p^{2j-d}$, recalling $N = p^d$. The number of k-asymmetric cycles must be non-negative for each k, so this model works for k such that

$$\frac{1}{k} > \frac{g/2+h/2+\gamma+\eta}{N} \tag{6.90}$$

or

$$k < \frac{N}{g/2+h/2+\gamma+\eta}. \tag{6.91}$$

Then we largest such k is

$$k_{max} = \left\lfloor \frac{N}{g/2+h/2+\gamma+\eta} \right\rfloor. \tag{6.92}$$

Equation (6.89) tells us that the number of k-cycles increases (or decreases) by a factor of p if we increase (or decrease) the number of integrals by one. We can sum k from 1 to $k_{\max}$ in (6.89) to obtain an estimate of the total number of asymmetric periodic cycles. Here we use the approximation that $k_{max} \approx \frac{N}{g/2+h/2+\gamma+\eta}$, to get

$$\#\text{asymmetric cycles} = \sum_{k=1}^{k_{max}} p^j \left(\frac{1}{k} - \frac{g/2+h/2+\gamma+\eta}{N} \right) \tag{6.93}$$

$$\approx p^j (H_{kmax} - 1) \tag{6.94}$$

$$\approx p^j \log \left(\frac{N}{g/2+h/2+\gamma+\eta} \right). \tag{6.95}$$

This means that we expect the number of asymmetric periodic cycles to increase by a factor of p for each additional integral present. This is significant for p of a reasonable

size. By making j the subject of (6.95) we obtain

$$\bar{j^*} = \frac{\log(\#\text{asymmetric cycles}) - \log\log\left(\frac{N}{g/2+h/2+\gamma+\eta}\right)}{\log p} \tag{6.96}$$

This gives us a test for j using the number of asymmetric cycles. Note we can't use any other type of orbit (symmetric periodic, symmetric aperiodic, asymmetric aperiodic) as a test as they are constrained by the fixed points and singular points whether there are integrals or not (see (8.4) and (8.5)). This result is useful because it can be used as a test for the number of integrals j of a reversible map without any a priori knowledge of the integrals or level sets. One concern of the model may be summing up values of k not in the allowed windows for period α but note that most of the sum is consumed by small k and larger values of k do not contribute much to the sum. Another concern may be the accuracy of this model as we have made some large assumptions and simplifications. However, it is quite robust, as additional integrals mean an increase of asymmetric cycles by factors of p. This means that if the model is out by a factor of $o(p)$, we should still be able to tell how many integrals it has.

This test is appropriate for reversible maps that have the same length cycles on level sets. However, we will see in chapter 8 a combinatorial model for reversible maps without integrals and in chapter 9 how we can generalise this to reversible maps with integrals (without the same length of cycles on level sets). In the end, we will see the model and the integral test give similar results for the expected number of asymmetric cycles and hence provide useful tests in any case. These two models will be compared in chapter 9 along with numerical tests showing its effectiveness.

6.7 Concluding Remarks

The presence of an integral affects the dynamics of a map over the finite field as the additional structure constrains the orbit structure. Through the example of the linear cat map and the QRT map, we showed the effects on the number of orbits and also the length of the orbits. In addition, for the QRT map, which is also reversible, we further considered the number of asymmetric orbits and provided a heuristic argument which may be used as a test to detect the number of integrals in higher dimensional reversible maps.

Chapter 7

Piece-wise Cat map

In this chapter, we study the periodic orbits of a three-parameter family of piecewise linear maps on the 2-torus. This map is invertible and for integer parameter values, the map preserves rational lattices and so each lattice decomposes into periodic orbits. We study the distributional properties of these periodic orbits on prime (rational) lattices and based on numerical evidence, we conjecture that asymptotically, almost all orbits are symmetric and for almost all parameter pairs, the distribution of normalised periods approaches the gamma distribution $\mathcal{R}(x) = 1-e^{-x}(1+x)$. Note that studying the rational orbits on prime lattices is equivalent to a study of the dynamics over the finite space $\mathbb{F}_p^2$. This had been conjectured by Roberts and Vivaldi for all reversible planar polynomial automorphisms with a single family of reversing symmetries on the finite space $\mathbb{F}_p^2$ [63] and shown to be the expected distribution for the composition of two involutions satisfying mild conditions on their fixed sets [64]. We also study parameter values for which this distribution is not followed. Some of these can be explained with knowledge about the action of toral automorphisms. In fact, when the parameter values are equal, we get precisely the action of toral automorphisms and hence we obtain a singular distribution for the period lengths of the orbits which was examined in the previous chapter 6.3.

7.1 Piecewise linear map

Consider area-preserving reversible maps of the form

$$L : x' = f(x) - y, \qquad y' = x \tag{7.1}$$

over some field K^2. This map is reversible for any choice of f, since we can write $L = H \circ G$, where

$$G : x' = x, \qquad y' = f(x) - y \qquad\qquad H : x' = y, \qquad y' = x. \tag{7.2}$$

It is easy to check that G and H are orientation-reversing involutions. Any 2nd order difference equation of the form

$$x_{n+1} = f(x_n) - x_{n-1} \tag{7.3}$$

can be written as the area-preserving reversible map in equation 7.1 by associating the points so that

$$(x_n, x_{n-1}) \leftrightarrow (x, y), \tag{7.4}$$

$$(x_{n+1}, x_n) \leftrightarrow (x', y'). \tag{7.5}$$

Here, we specialize the map L to be a three parameter family of piece-wise linear maps T of the two-dimensional torus $\mathbb{T}^2$, where f in (7.1) is given by

$$f(x) = \begin{cases} bx & \text{if } x \in [0, s) \\ ax & \text{if } x \in [s, 1) \end{cases} \tag{7.6}$$

where a, b are integers and $s \in [0, 1)$. This map can be seen to be a very simple area-preserving and non-trivial perturbation of the map (6.14). This map can also be written as

$$T(x, y) = \begin{pmatrix} \theta(x) & -1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix} \pmod 1, \tag{7.7}$$

where

$$\theta_{ab}(x) = \begin{cases} b & \text{if } x \in [0, s) \\ a & \text{if } x \in [s, 1). \end{cases} \tag{7.8}$$

We will study the idea of reversibility through this mapping. This property should be thought of as a global algebraic property and we will see how the period structure in finite representations can be used to identify it. Thus, we are interested in studying the rational periodic orbits of T. Note that all rational points on the torus are periodic. This

is easily seen by considering the orthogonal rational lattice with N^2 points, Λ_N, on the torus defined by

$$\Lambda_N = \{(\tfrac{i}{N}, \tfrac{j}{N}) \mid i, j \in \mathbb{Z}_N\}, \qquad N \in \mathbb{Z}^+. \tag{7.9}$$

Now Λ_N is finite and invariant under T and since T is invertible, then each point in Λ_N is periodic under T. For a fixed rational lattice Λ_N, we can consider the cumulative distribution function of the period for all the N^2 points given by:

$$\mathcal{D}_N(x) = \frac{\#\{z \in \Lambda_N \mid t(z) \leq \kappa x\}}{N^2} \tag{7.10}$$

where constant κ is a normalisation parameter. $\mathcal{D}_N(x)$ represents the proportion of points in Λ_N that have period less than or equal to κx. Since $t(z)$ is an integer, the function $\mathcal{D}_N$ is a step function where the number of steps is equal to the number of distinct periods of T over Λ_N. Note that the distribution function is dependent on the parameter choices a, b, s. This periodic distribution function has been studied [63, 52] for various maps of finite spaces including the area-preserving Hénon map. The following was conjectured in [63]:

Conjecture 7.1.1. *For a reversible polynomial automorphism (with a single family of reversing symmetries) acting on a space $\Lambda_p \cong \mathbb{F}_p^2$ then*

$$\lim_{p\to\infty} \mathcal{D}_p(x) = \mathcal{R}(x) = 1 - e^{-x}(1 + x) \qquad x \geq 0 \tag{7.11}$$

where the normalisation parameter is taken to be the mean period, that is,

$$\kappa = \frac{p^2}{\#\text{cycles}}. \tag{7.12}$$

The distribution function $\mathcal{R}(x)$ is the cumulative distribution function of the gamma function with shape parameter 2 and scale parameter 1. This distribution has been shown to be the expected limiting distribution of the composition of two random involutions with some conditions on the cardinality of their fixed sets [64]. This suggests that the convergence of the period distribution to $\mathcal{R}(x)$ may be enough to infer reversibility over a finite space. Referring back to (7.1), one might ask which functions f will see the asymptotics (7.11). For $f(x) = x^2 + \epsilon$ (the area preserving Hénon map), there is strong evidence that it follows the gamma distribution [63]. For linear functions $f(x) = cx, c \in \mathbb{N}$, we obtain singular distributions corresponding to hyperbolic toral automorphisms which

was categorised in [55]. In fact under T, if $a = b$ or $s = 0$, then we obtain the linear map on the torus

$$T(x, y) = \begin{pmatrix} a & -1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix} \pmod 1. \tag{7.13}$$

Thus the map T, a three parameter family of piece-wise linear maps can be seen as a small deviation from linear toral automorphisms which motivates the study of this map. In section 7.3.1, by fixing a, b, p and considering small values of s, we will see the gradual departure of $D_p(x)$ from the singular distribution to $\mathcal{R}(x)$.

We will study the convergence of the distribution function $\mathcal{D}_N$ for T when $N = p$ is a prime number. For some special parameter pairs, we will see that the period distributions differ from $\mathcal{R}(x)$. We are interested in the convergence of the period distribution of $\mathcal{R}(x)$ and we will provide evidence using "large" primes p and by examining the norm of the difference $|\mathcal{D}_p - \mathcal{R}|$ as a function of the parameters of the map. Figure 7.1 is a plot of the distribution function $D_N(x)$ for various primes N which provides preliminary evidence for a similar result to conjecture 7.1.1 for the map (7.7). Thus we present the following conjecture:

Conjecture 7.1.2. *The cumulative distribution function of the map T of (7.7) for fixed a, b, s where $s \neq 0$ and $a \neq b$ has limiting distribution*

$$\lim_{N\to\infty} \mathcal{D}_N(x) = \mathcal{R}(x) = 1 - e^{-x}(1 + x) \qquad x \geq 0 \tag{7.14}$$

where the normalisation parameter is taken to be the mean period, that is,

$$\kappa = \frac{p^2}{\#cycles}. \tag{7.15}$$

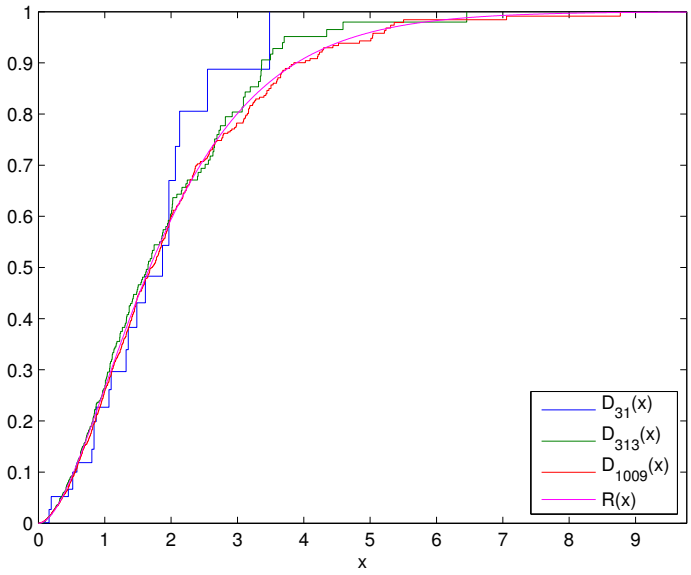


Figure 7.1: Plot of the distribution of cycle lengths $\mathcal{D}_N(x)$ of (7.10) and the conjectured distribution $\mathcal{R}(x)$ for $p = 31$, $p = 313$ and $p = 1009$ with parameters $a = 13, b = 7, s = 0.5$ in (7.7). We have $\mathcal{E}_{31}(a,b) = 0.373562712177397, \mathcal{E}_{313}(a,b) = 0.122287773626187$ and $\mathcal{E}_{1009}(a,b) = 0.060146308097751$ where $\mathcal{E}(a,b,s)$ is defined in (7.26).

7.2 Reversibility and symmetry of piece-wise linear map

The family of maps (7.7) can be written as the composition of two involutions, that is, $T = H \circ G$ where

$$G : x' = x, \qquad y' = \theta_{ab}(x)x - y \qquad\qquad H : x' = y, \qquad y' = x. \tag{7.16}$$

Now consider the fixed sets of the involutions G, H given by

$$\mathrm{Fix}(G) = \{(x,y) : 2y = \theta_{ab}(x)x\}, \qquad \mathrm{Fix}(H) = \{(x,y) : x = y\}. \tag{7.17}$$

These are one-dimensional curves on the torus and classify the symmetric orbits.

We now focus our study of T to the rational lattice Λ_N. By clearing the denominator in (7.9) we obtain the integer lattice of the numerators which we still denote by Λ_N. The action of T on the rational lattice Λ_N can now be described by the permutation (with abuse of notation we also call it T and henceforth T refers to the below mapping) T given by

$$T : x' = \theta_{ab}^N(x)x - y \pmod N \qquad y' = x \pmod N \tag{7.18}$$

where we identify x, y with their respective numerators over the denominator N, so in (7.18) we have $x, y \in \mathbb{Z}_N$ and

$$\theta_{ab}^N(x) = \begin{cases} b & x \in \{0, 1, \ldots, \lceil Ns \rceil - 1\} \\ a & x \in \{\lceil Ns \rceil, \ldots, N-1\}. \end{cases} \tag{7.19}$$

Note that for $s = 0$, we get exactly the dynamics of the linear map on the torus. This behaviour has been documented in section 6.3. However (for $a \neq b$), increasing s to a non-trivial value "perturbs" the structure of the map, at first minimally, but we will see entirely different cycle structure. This will be discussed in section 7.3 and motivates the study of this map. The map T acquires the corresponding reversibility (7.17) with

$$\begin{aligned} \mathrm{Fix}(H) &= \{(x, x) \mid x \in \mathbb{Z}_N\} \\ \mathrm{Fix}(G) &= \{(x, y) \mid 2y = \theta_{ab}^N(x)x \pmod N\}. \end{aligned} \tag{7.20}$$

Here, $\mathrm{Fix}(H)$ are the integer coordinates $(\mathrm{mod}\, N)$ on the line $x = y$ while $\mathrm{Fix}(G)$ is the union of two half lines. Now over a finite space with invertible mapping T, all points are periodic. We consider the symmetric periodic orbits, that is, those that intersect $\mathrm{Fix}(G) \cup \mathrm{Fix}(H)$.

When N is odd, 2 has a modular inverse and $\mathrm{Fix}(H), \mathrm{Fix}(G)$ each have N points. We obtain the following bound on the number of cycles of L,

$$\frac{\#\mathrm{Fix}(G) + \#\mathrm{Fix}(H)}{2} = N = \#\mathrm{SymCycles}(L) \leq \#\mathrm{Cycles}(L) \tag{7.21}$$

from theorem 5.3.2. In practice, we see very few asymmetric cycles and they seem to play no part in the asymptotics of the distribution of the cycles.

Below we will prove that there is also a reflection in the parameter space where we write $\theta_{a,b,s}^N$ to differentiate θ^N with different parameter values.

Lemma 7.2.1. *For $\theta_{a,b,s}^N(x)$ defined in (7.19), we have $\theta_{a,b,s}^N(x) = \theta_{b,a,1-s}^N(-x)$ for $x \neq 0$.*

Proof. Suppose $x \in \{1, \ldots, \lceil Ns \rceil - 1\}$ so $\theta_{a,b,s}^N(x) = b$. Then working modulo N it is clear that $-x \in \{N - \lceil Ns \rceil + 1, \ldots, N-1\}$. But for $N \geq \lceil Ns \rceil \geq 0$ and $Ns \notin \mathbb{Z}$, we have

$N - \lceil Ns \rceil + 1 = \lceil N - Ns \rceil = \lceil N(1-s) \rceil$, then

$$\theta^N_{a,b,s}(x) = b = \theta^N_{b,a,1-s}(-x). \tag{7.22}$$

Similarly for $x \in \{\lceil Ns \rceil \dots N-1\}$ and thus the relation is clear. □

We now write $T_{a,b,s}$ to refer to the map T with parameters a, b, s for convenience.

Claim 7.2.2. The distribution of orbits under $T_{a,b,s}$ is the same as that under $T_{b,a,1-s}$, that is, $\mathcal{D}_{p,a,b,s}(x) = \mathcal{D}_{p,b,a,1-s}(x)$.

Proof. We prove this by showing that $T_{a,b,s}$ and $T_{b,a,1-s}$ are conjugate. Consider the mapping $h : \mathbb{Z}_N^2 \to \mathbb{Z}_N^2$ where $h = -Id$. Noting that $h = h^{-1}$, we can write

$$T_{b,a,1-s} \circ h = h^{-1} \circ T_{a,b,s} \tag{7.23}$$

since for $x \neq 0$ we have

$$\begin{aligned} T_{b,a,1-s} \circ h(x,y) = T_{b,a,1-s}(-x,-y) &= \begin{pmatrix} \theta^N_{b,a,1-s}(-x) & -1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} -x \\ -y \end{pmatrix} \\ &= \begin{pmatrix} \theta^N_{a,b,s}(x) & -1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} -x \\ -y \end{pmatrix} \qquad \text{by lemma (7.2.1)} \\ &= h \circ T_{a,b,s}(x,y) \end{aligned} \tag{7.24}$$

and for $x = 0$, (7.23) is clearly true. Thus, we have the one-to-one parameter relation for the nth iterates of the T_N,

$$(T_{a,b,s})^n = h^{-1} \circ (T_{b,a,1-s})^n \circ h \tag{7.25}$$

for $n \in \mathbb{Z}^+$ which complete the proof. □

In particular from the above claim, if we set $s = 1/2$ and for a fixed odd N consider the value of $\mathcal{D}_{N,a,b,s}(x)$ for all parameters a, b, we need only look at values $\{(a,b) \mid b \leq a\}$.

7.3 Evidence for convergence to $\mathcal{R}(x)$ for almost all parameters

We now provide experimental evidence and results for the mapping T and take $N = p$ a large prime. In order to quantify convergence, we define a function to measure the distance between the conjectured distribution $\mathcal{R}(x)$ and the empirical distribution function $\mathcal{D}_p(x)$. We use the L^1-norm and define the error function $\mathcal{E}_p(a, b, s)$ as:

$$\mathcal{E}_p(a, b, s) = \int_0^\infty |\mathcal{D}_{p,a,b,s}(x) - \mathcal{R}(x)|dx. \tag{7.26}$$

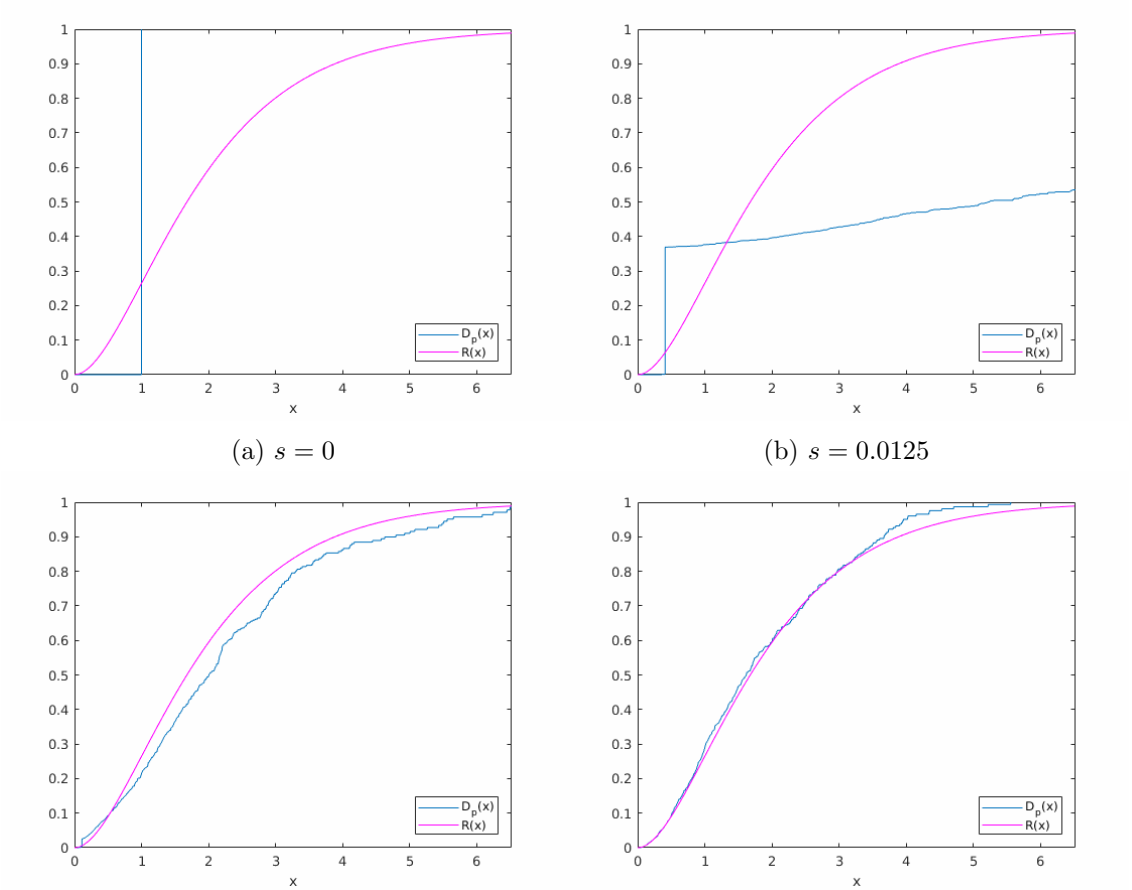
A restatement of conjecture 7.1.1 applied to the map T is that for all fixed a, b, s (such that T has a single family of reversing symmetries) we have

$$\lim_{p\to\infty} \mathcal{E}_p(a, b, s) = 0. \tag{7.27}$$

The case for $a = b$ or $s = 0$ reduces to the linear map which was studied in chapter 6.3 and has more than a single family of reversing symmetries.

7.3.1 Increasing s (fixed a,b,p)

As we increase s slightly, visually we can see the change from the singular distribution corresponding to $s = 0$ to the gamma distribution $\mathcal{R}(x)$. The change of value in s from 0 perturbs the linear structure of the toral automorphism and brings a different structure and period distribution. We see the effects of small increases in s in figure 7.2 for fixed a, b, p. The top left frame is for $p = 821, a = 123, b = 379, s = 0$, with all points period 82 except for fixed point at the origin. In the subsequent subfigures, as the value of s increases slightly, we continue to see a "spike" in the distribution where a large proportion of points have the same period 82. Indeed, the repeated period is the same for each subfigure and in each subsequent figure is a smaller subset of orbits of this period from the previous subfigure. This is because increasing s (slightly) to $s' = s + \epsilon$ does not affect those orbits that have $x > s'$ for each point. This is also shown in figure 7.3 where our distribution functions are shown without scaling. Here we see the common spike at 82 decreases with the increase of s. As s increases, we slowly filter out these repeated periods from the linear map and as they disappear, we see that the distribution of the periods moves closer to the conjectured distribution $\mathcal{R}(x)$. We can see the rate of this by plotting the "spike" for



(a) $s = 0$ (b) $s = 0.0125$

(c) $s = 0.00499$ (d) $s = 0.1122$

Figure 7.2: Plots of $\mathcal{D}_p(x)$ for fixed $p = 821, a = 123, b = 379$ and varying s.

every value of s. Formally, for fixed p, a and $b = a$ (where x_n represents the x coordinate of the nth iteration), we define $f(s)$ as:

$$f(s) = \frac{\{(x_0, y_0) \mid x_n > s \text{ for all } n \geq 0\}}{p^2} \tag{7.28}$$

which represents the proportion of space with orbits fully contained in $(s, 1) \times [0, 1)$ for $s \in [0, 1)$. By assuming spatial equidistribution of the points in orbits [16], we can estimate $f(s)$ using a probabilistic approach. To see a (repeated) orbit under T, each point must be in the region $(s, 1) \times [0, 1)$. Now take the common period length to be t then,

$$\mathbb{E}[f(s)] = (1 - s)^t. \tag{7.29}$$

This is shown in figure 7.4 where the blue line is $f(s)$ and the magenta line is $\mathbb{E}[f(s)] = (1 - s)^t$.

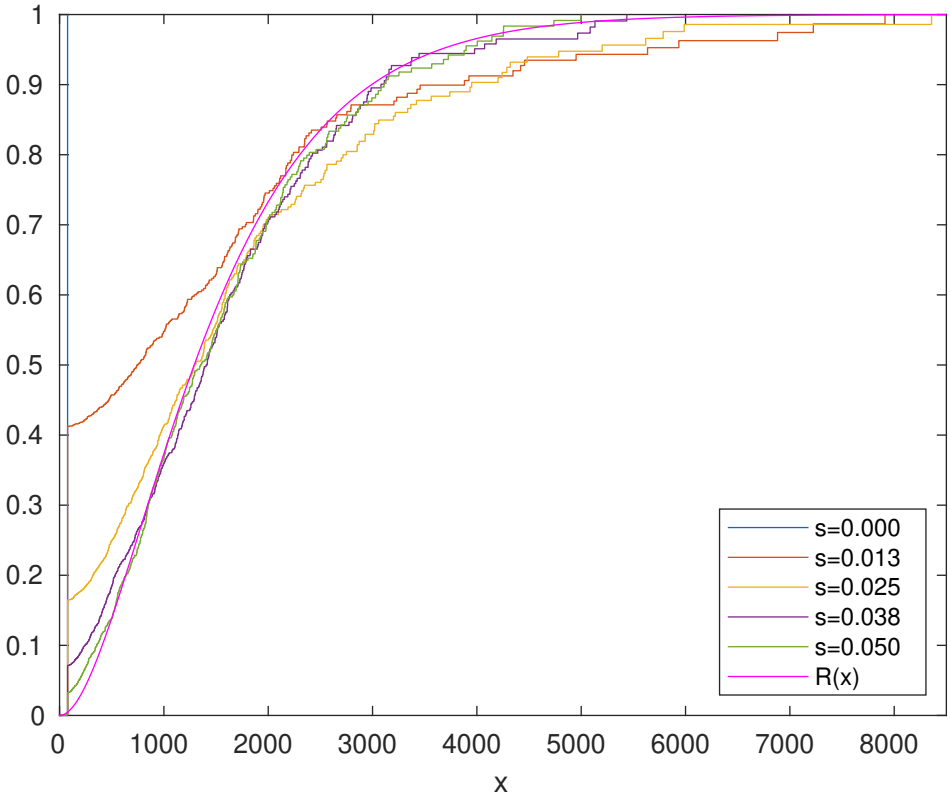


Figure 7.3: Plot for $p = 769, a = 23, b = 442$ and changing s with no scaling by κ.

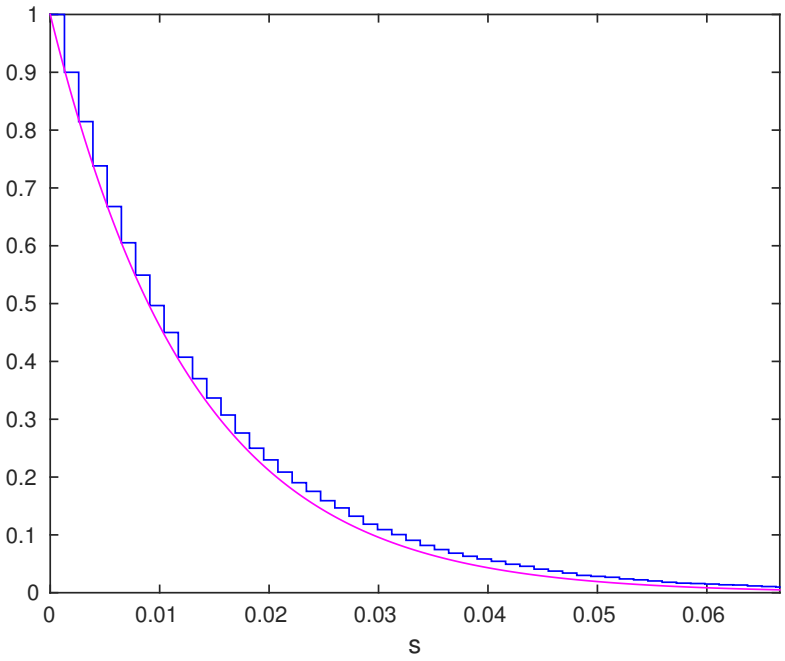


Figure 7.4: Proportion of orbits that stay in region $(s, 1)\times[0, 1)$ as s varies for $p = 769, a = 23, b = a$

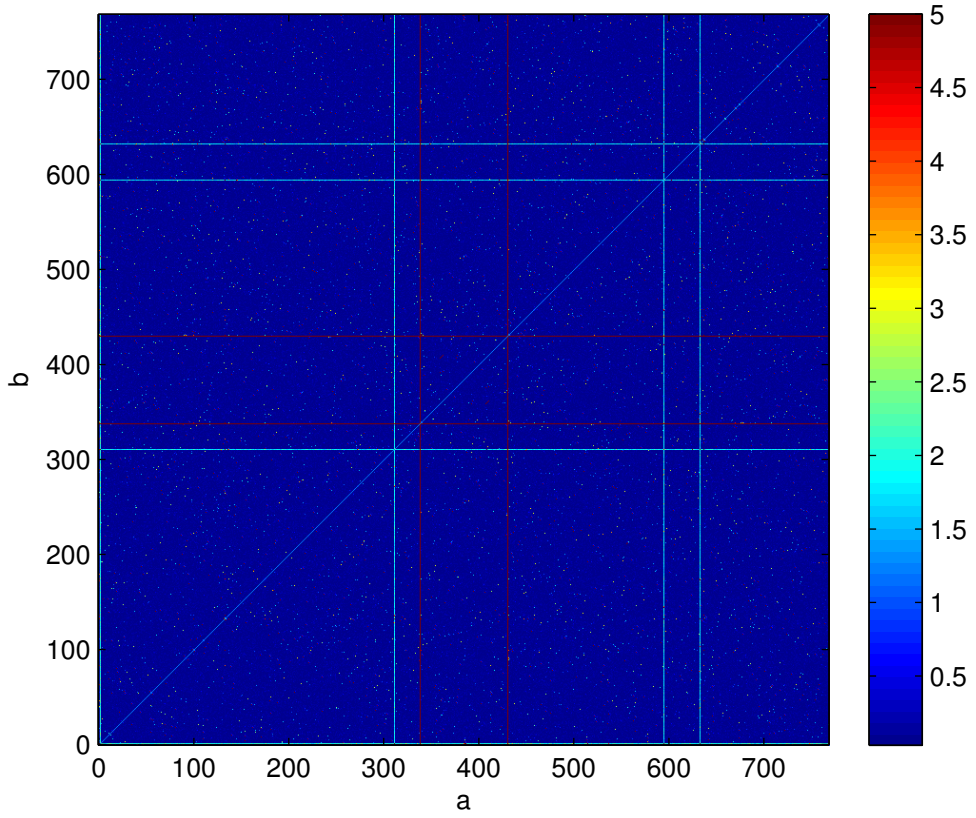


Figure 7.5: Plot of error $\mathcal{E}_p(a, b, s)$ of (7.26) capped at 5 with $p = 769$ with $s = 0.5$ for parameter space a, b.

7.3.2 Varying a,b (fixed s,p)

One way we can explore convergence of $\mathcal{E}_p(a, b, s)$ is by fixing s and (a large) p and considering its value over all parameters a, b. We can represent this pictorially through a $p \times p$ image of boxes where each box is shaded corresponding to its value of $\mathcal{E}_p(a, b, s)$ as shown in figure 7.5 for $p = 769, s = 0.5$. There, the value is represented by the colour bar on the right which we have capped at 5 because we are mainly concerned with convergence. Here, small deviations from the gamma distribution are in dark blue, while large deviations are shown in dark red. Representing the distance for $\mathcal{R}(x)$ in this way can be helpful to identify (linear) patterns in (a, b) parameter space. This computation is not trivial as for a fixed p, we find the period distributions for the p^2 parameter pairs where each is over a space of p^2 points. Thus computation increases proportional to p^4. Savings in computation can be made by exploiting parameter symmetry and by searching along the symmetry lines for symmetric orbits. To analyse the convergence for parameter

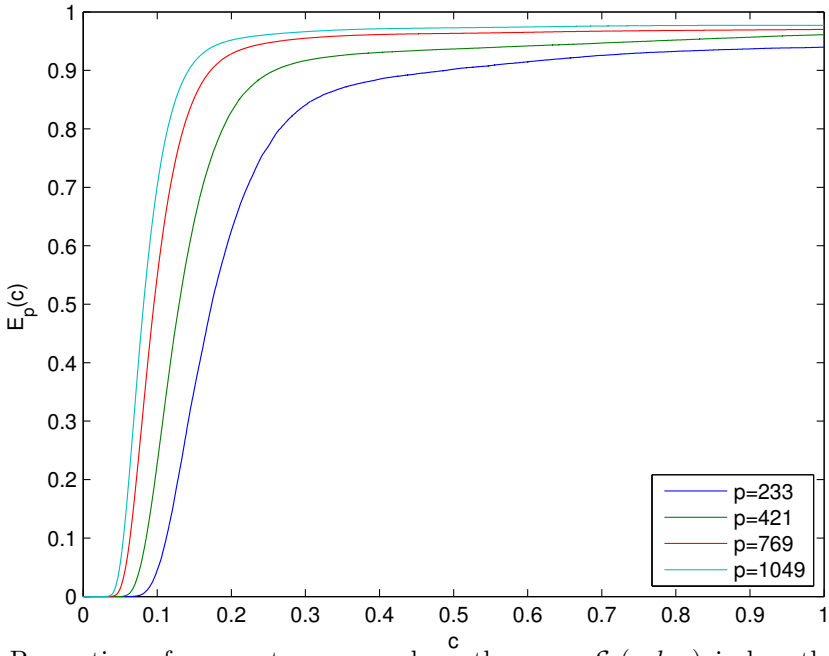


Figure 7.6: Proportion of parameter space where the error $\mathcal{E}_p(a, b, s)$ is less than c for $p = 233, 421, 769, 1049$ for $s = 0.5$.

values as a whole, we define the following function,

$$E_{p,s}(c) = \frac{\#\{(a, b) \in \Lambda_p \mid \mathcal{E}_p(a, b, s) < c\}}{p^2}. \tag{7.30}$$

This is the proportion of parameter pairs for which the period distribution has distance less than c from $\mathcal{R}(x)$. For some fixed p and s, this is also a distribution function as it is non-decreasing in c and is equal to 1 for sufficiently large c. Figure 7.6 shows the plot of $E_{p,s}(c)$ for 4 values of p. We see that for fixed c and increasing p with $s = 0.5$, the proportion of parameter pairs that have error value $\mathcal{E}_p(a, b, s)$ less than c seems to increase. This leads us to define

$$E_s(c) = \liminf_{p\to\infty} E_{p,s}(c) \qquad c > 0. \tag{7.31}$$

The function E_s is non-decreasing and numerical evidence suggests the following:

Conjecture 7.3.1. *The function E_s is identically equal to 1.*

This conjecture states that for almost all parameter pairs (fixed p, s), the period distribution of the rational cycles of T_p is the same as the gamma distribution. (By construction, the function E_s is not affected by anomalous distributions which may appear for sets of parameters of size $o(p^2)$.)

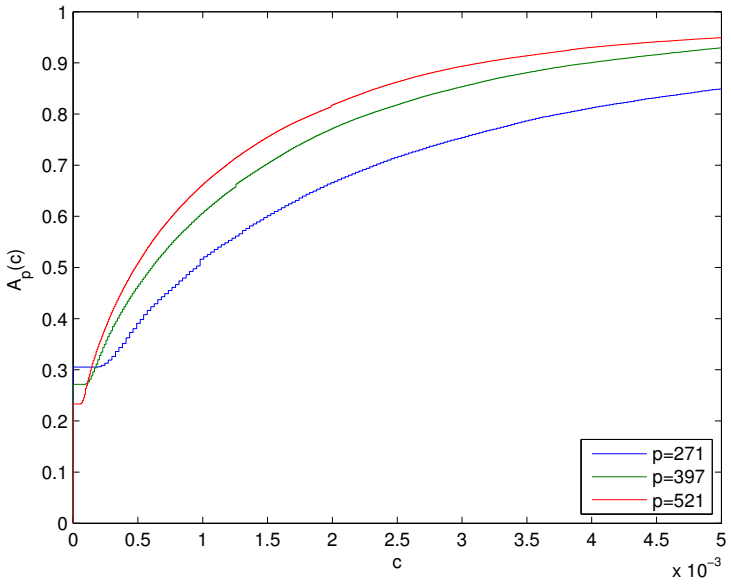


Figure 7.7: Proportion of parameter space where the space taken up by asymmetric orbits is less than c. Note the scale of the x-axis.

In [63] is was shown that for random reversible maps, asymptotically, asymmetric cycles have zero probability. Here, we provide evidence that T_N shares this same property. For T_N we consider the proportion of points (x, y) on the rational lattice which belong to asymmetric periodic orbits. Then we define

$$\mathcal{A}_p(a, b, s) = \frac{\#\{(x, y) \in \Lambda_p \mid (x, y) \text{ belongs to an asymmetric cycle}\}}{p^2}. \tag{7.32}$$

We also fix a constant $c > 0$ and define

$$A_{p,s}(c) = \frac{\#\{(a, b) \mid \mathcal{A}_p(a, b) < c\}}{p^2} \tag{7.33}$$

which is the proportion of parameter pairs for which the proportion of asymmetric points is less than c. This function is non-decreasing and equal 1 for $c \geq 1$. Now define

$$A_s(c) = \liminf_{p\to\infty} A_p(c), \qquad c \geq 0. \tag{7.34}$$

Conjecture 7.3.2. *The function A_s is identically equal to 1.*

Figure 7.7 provides numerical evidence for this conjecture. For example, we see that for $p = 521$ and $c = 0.005$, we have that 257661 out of the $521^2 = 271441$ or 94.92% of the parameter pairs have asymmetric cycles taking up less than 0.5% of the phase space.

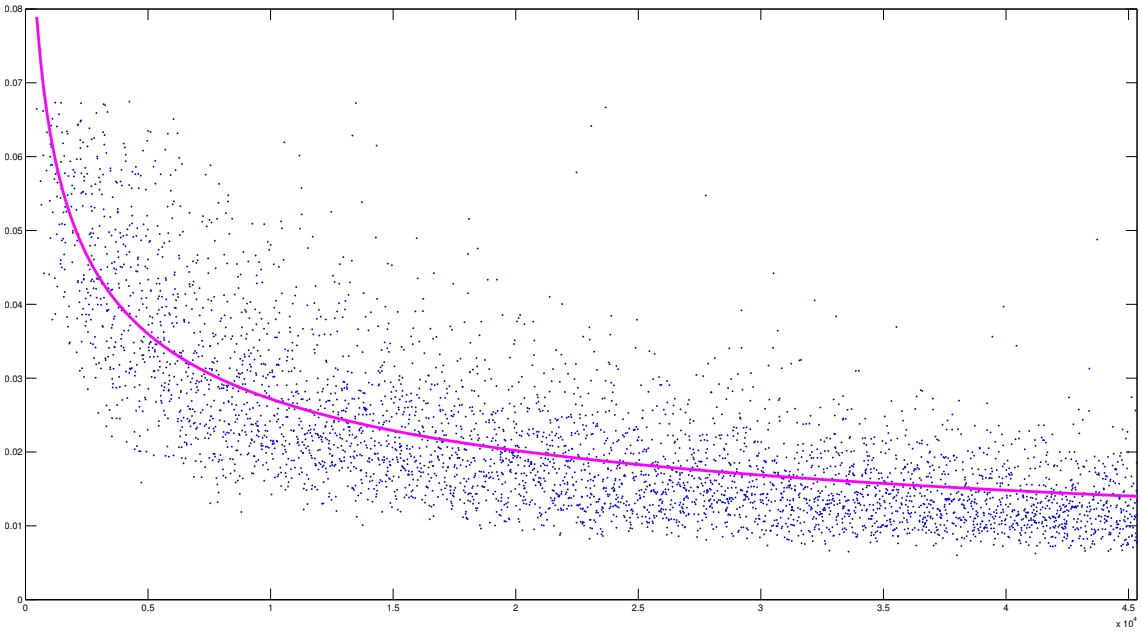


Figure 7.8: Plot of error for $a = 123, b = 421$ and all primes from $p = 431$ to 45343 with the curve $y = \frac{1}{0.3309\sqrt{p}+5.229}$ (a curve of best fit).

7.3.3 Varying p (fixed a,b,s)

We can also fix a, b, s and observe this error function $\mathcal{E}_p(a, b, s)$ for increasing p. This is shown in figure 7.8. We calculated the error function $\mathcal{E}_p$ for all primes $p = 431$ to 45343 with $a = 123, b = 421, s = 0.5$. To fit this curve, we used least squares (and trimming). The error $\mathcal{E}_p(a, b) = O(\frac{1}{\sqrt{p}})$. This gives us an approximate rate of convergence as $p \to \infty$.

7.4 Anomalous distributions for fixed p

In this section, we discuss various parameter values for fixed p where the value of $\mathcal{E}_p(a, b, s)$ of (7.26) is "large". For these parameter values, we are typically seeing many asymmetric cycles, many with the same small cycle length. Note that this does not contradict conjecture 7.1.2 as we still believe that as $p \to \infty$, the distribution has the expected convergence. However, this also means that the convergence is not uniform as even for large values of p, some parameter values will have a "large" error. We describe some specific examples of the parameter values where this occurs and present necessary conditions for this. Now, for fixed p and s, we can separate the parameters in which anomalous distributions occur into two types:

1. Occurs for a particular a and for all b (independent of b).

2. Occurs for particular combinations a, b.

Type 1: We can see type 1 in figure 7.5, in the horizontal and vertical lines for $s = 0.5$. (Since this is symmetric with respect to the axes, we concentrate without loss of generality on the vertical lines.) For the values of a corresponding to vertical lines, this is related to the linear map in (6.14). There we saw that for $s = 0$, the distribution was singular with all orbits having the same period length, and as s increased, the distribution became closer to $\mathcal{R}(x)$. These occur when many of the orbits have points entirely on one side of the switch s. The rate of this is dependent on the value of the common period t in the linear case. For parameter values a corresponding to small common period t (section 3.1, theorem 3.1), the proportion of space occupied by these common cycles can be approximated by $(1 - s)^t$. In this case, the distribution will have a spike at this value which leads to a larger error when compared to the "average" parameter pair (a, b). The abundance of small cycles also affects the scaling factor κ.

Type 2: Parameter combinations for type 2 cover the rest of the anomalous distributions. The parameters a, b that fall under this category satisfy some special relation that causes the many small repeated cycles to occur. These are different to those in type 1 because the small cycle orbits in this case will have points on both sides of the switch. In contrast to type 1, as s becomes closer to 0 (from 1/2), the number of these small cycles will decrease.

We can see examples of both types of anomalous distribution in figure 7.9. Type 1 are the horizontal and vertical lines while type 2 are the lines with gradient 1,2 or 3. The latter correspond to parameters a, b satisfying $ab = 1, 2, 3 \pmod p$ respectively. Note that the density of these anomalous distribution goes to 0 as $p \to \infty$ (see conjecture 7.3.1).

In figure 7.9 for $p = 769$ we can see horizontal lines corresponding to type 1 errors at $a = 2, 311, 338, 430, 594, 632, 768$.

Example 7.4.1. If we look into the periodic orbits of $T_{a,b,s}$ for $a = 338 = b$ on Λ_{769}, we see that there are 118272 distinct orbits with period length 5. We also find that 3696 of these orbits have a spatial distribution confined to $[\frac{1}{2}, 1) \times [0, 1)$. This tells us that the mapping $T_{a,b,s}$ with $a = 338, s = 0.5$ will have at least 3696 distinct orbits of period 5 for independent of b.

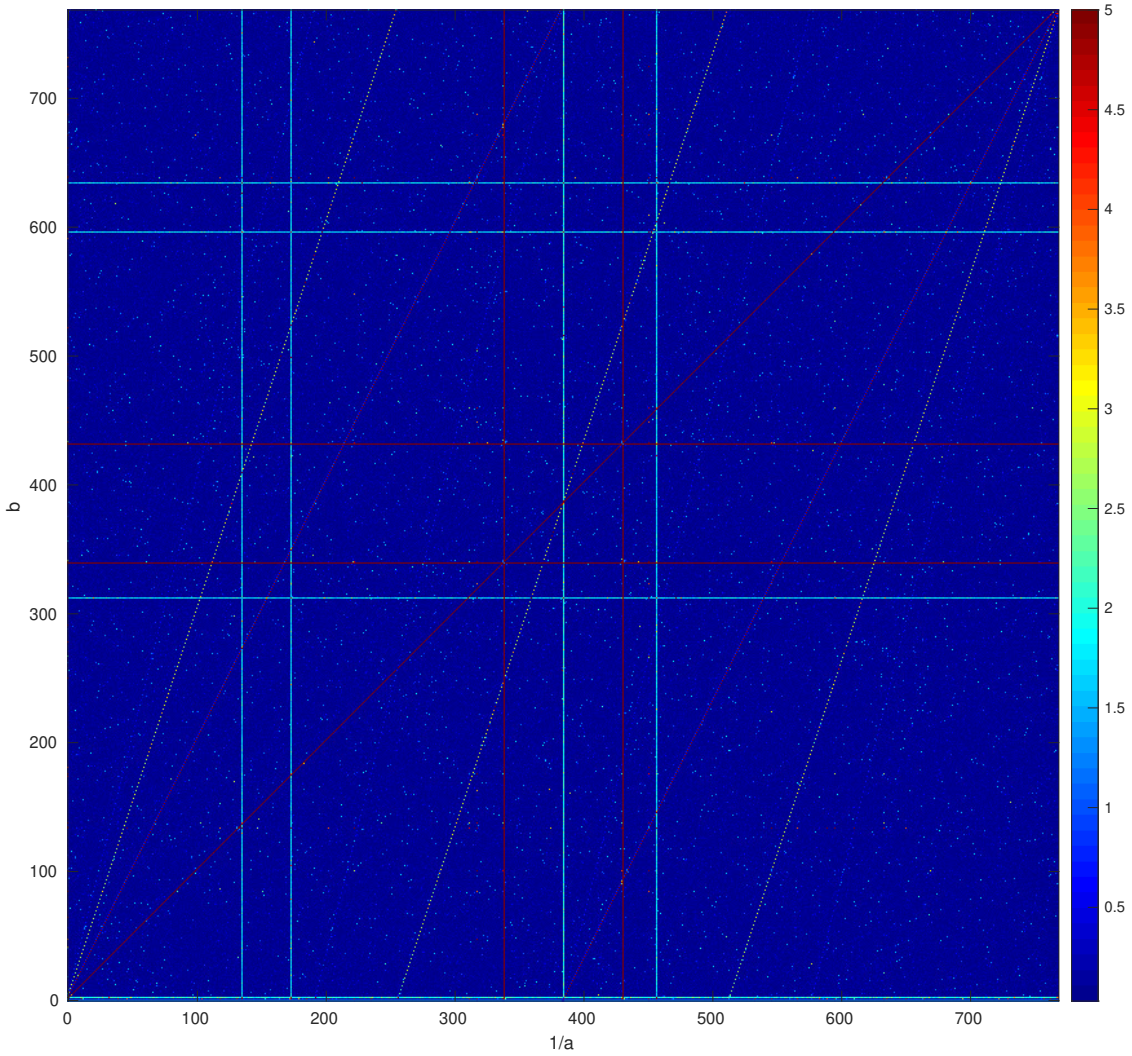


Figure 7.9: Plot of error $\mathcal{E}_p(1/a, b, s)$ capped at 5 with $p = 769, s = 0.5$ for parameter space $1/a, b$ showing a hyperbolic relation.

7.4.1 Words and matrix words

To better understand the nature of these anomalous parameter values we introduce some notation. We will associate each point $z = (x, y)$ with a "word" consisting of a sequence of letters in $\{a, b\}$. Let us denote the word of a point $z = (x, y)$ by ω. We define θ as

$$\theta(x) = \begin{cases} b & x \in [0, s) \\ a & x \in [s, 1) \end{cases} \tag{7.35}$$

and we build a word where the $(k+1)$th letter is given by $\theta(x_k)$ where $(x_k, y_k) = T^k(x_0, y_0)$ and here we regard b, a as letters rather than as parameter values. We write the letters in our word from right to left, that is, a word of length n will have word $\omega =$

$\theta(x_{n-1})\theta(x_{n-2})\dots\theta(x_0)$. If a point z has period n then its associated word can be represented with n letters. Then points in the same orbit will have words that are cyclic permutations. Suppose (x, y) has associated word $\omega_{x,y}$ of length n and denote the kth letter of the word by c_k. We define an associated matrix word $\Omega_{x,y} = C_n C_{n-1} \dots C_1$ where

$$C_k = \begin{cases} B & c_k = b \\ A & c_k = a \end{cases} \tag{7.36}$$

and

$$A = \begin{pmatrix} a & -1 \\ 1 & 0 \end{pmatrix} \qquad B = \begin{pmatrix} b & -1 \\ 1 & 0 \end{pmatrix}. \tag{7.37}$$

Now recall that for a point (x, y) to be periodic with period n, we must have

$$T^n(x, y)^T = (x, y)^T. \tag{7.38}$$

Then we also have that

$$\Omega_{x,y}(x, y)^T = (x, y) \pmod 1 \tag{7.39}$$

where $\Omega_{x,y} \in SL(2, \mathbb{Z})$. Now consider solutions (x, y) in Λ_p the rational lattice with prime denominator p. Since $\Omega_{x,y}$ is an integer matrix, this induces modulo p arithmetic so that

$$(\Omega_{x,y} - Id)(x, y)^T = \mathbf{0} \pmod p \qquad x, y \in \mathbb{F}_p. \tag{7.40}$$

If $\Delta = \det(\Omega_{x,y} - Id) = \det(\Omega_{x,y}) - \text{trace}(\Omega_{x,y}) + 1 \neq 0$, then using Cramer's rule the only solution is the trivial solution. So, every non-trivial point (x, y) in Λ_p has a corresponding matrix word $\Omega_{x,y}$ that satisfies $\text{trace}(\Omega_{x,y}) = \det(\Omega_{x,y}) + 1 = 2$. Now for a given word $w_{x,y}$ and corresponding matrix word $\Omega_{x,y}$, we may want to find all $(x', y') \in \Lambda_p$ that have word $w_{x,y}$. A necessary condition is that it must satisfy (7.40). For non-trivial solutions, the dimension of $\ker(\Omega_{x,y} - Id)$ must be 1 or 2. If the dimension of $\ker(\Omega_{x,y} - Id) = 1$ then there are p possible solutions while if $\ker(\Omega_{x,y} - Id) = 2$, then every lattice point is a possible solution. However, for a point (x', y') to be a valid solution to (7.40), we must also have $w_{x,y} = w_{x',y'}$. Let us call words $\omega_{x,y}$ that have $\dim(\ker(\Omega_{x,y} - Id)) = 2$ *singular words*. A singular word is equivalent to having $\Omega_{x,y} = Id \pmod p$. When $s = 0$, every point has the same singular word of length t, consisting entirely of the letter a. As we increase s, the word of each point may or may not change, and for small t the proportion

that keep the initial word is approximately $(1-s)^t$. When there is an (x, y) with singular word of short length n, the distance of the period distribution from $\mathcal{R}(x)$ will be large. This is because there will be many small orbits with the same singular word. The number is dependent on the value of s. In general, for a fixed p, we observe the following:

1. The number of points with singular words in type 1 error parameters decreases as s increases (from 0 to 0.5).
2. The number of points with singular words in type 2 error parameters increases as s increases (from 0 to 0.5).

We can see the manifestation of (1) in figure 7.3 and 7.4. This phenomenon is clear because f in (7.28) is a non-increasing function. For (2) we have provided evidence that show this general trend in figure 7.10 although in this case it is not strict as in figure 7.10b and 7.10c we see that the peak is not at $s = 0.5$.

For some parameter values, we see some patterns in the words that occur. In particular for some anomalous distribution we saw common words for different prime lattices. Now we will look at some examples of these words and describe some parameter values where they occur and hence where we see anomalous distributions. These are some examples of parameters with type 2 error along with their singular words. For a fixed p and parameter pair in the set $\{(a, b) : ab = 1, 2, 3 \pmod p\}$, there exist singular words of length $6, 8, 12$ corresponding to $ab = 1, 2, 3 \pmod p$ respectively. We will state the words explicitly and study the proportion of space occupied by these words for $s = 0.5$.

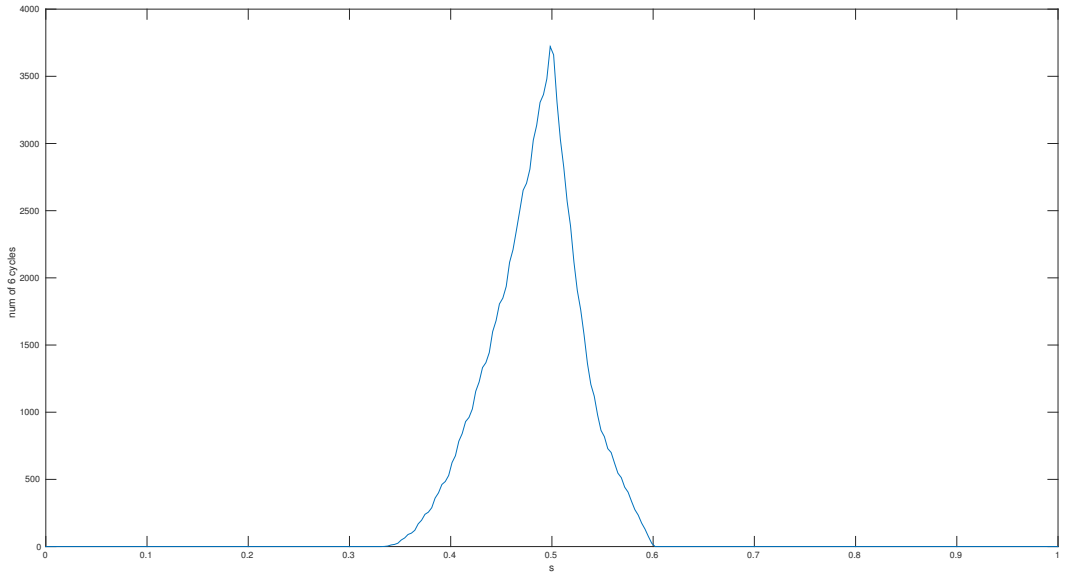
- For parameters satisfying $ab = 1 \pmod p$ there exists singular words *bababa*.
- For parameters satisfying $ab = 2 \pmod p$ there exists singular words *bbabaaba*.
- For parameters satisfying $ab = 3 \pmod p$ there exists singular words *bbababaababa*.

Consider the word $w = bababa$. Then the corresponding matrix word $\Omega = BABABA$ is

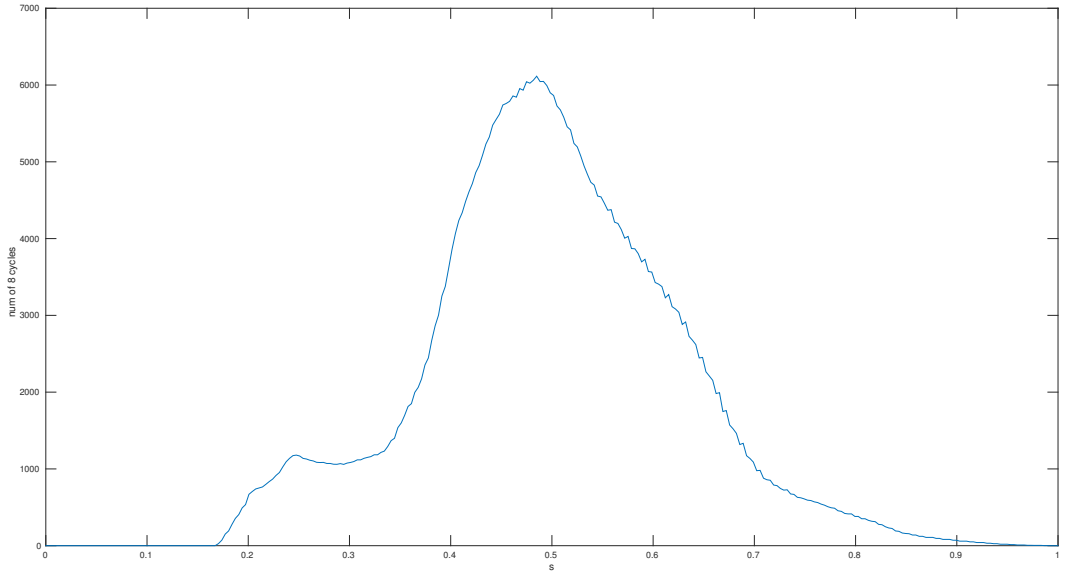
$$\Omega = \begin{pmatrix} a^3b^3 - 5a^2b^2 + 6ab - 1 & -a^2b^3 + 4ab^2 - 3b \\ a^3b^2 - 4a^2b + 3a & -a^2b^2 + 3ab - 1 \end{pmatrix} \tag{7.41}$$

and

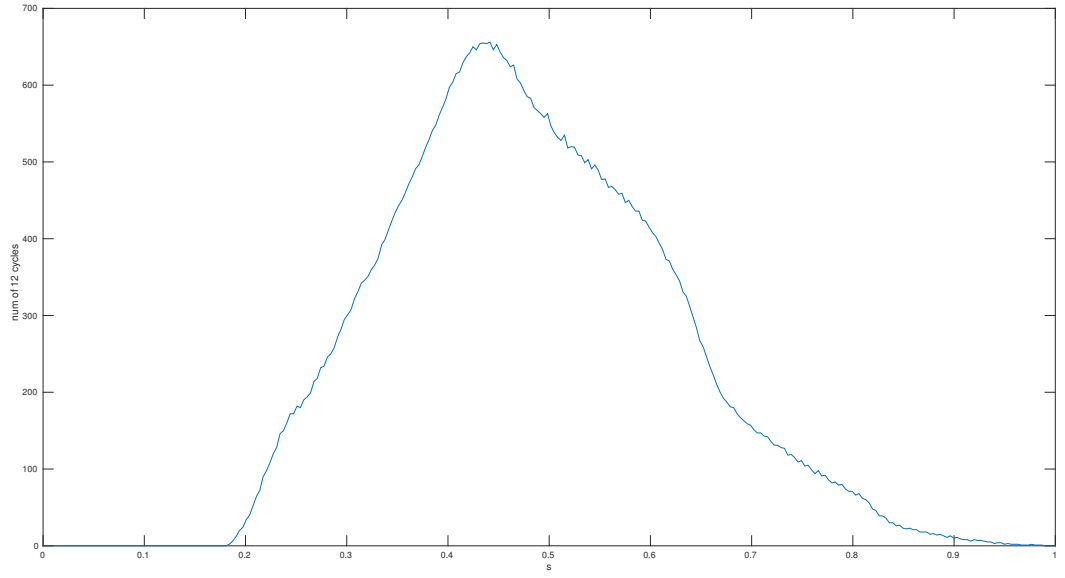
$$\text{trace}(\Omega) - 2 = (ab - 4)(ab - 1)^2. \tag{7.42}$$



(a) Plot of number of 6 cycles as the switch changes for $p = 613, a = 5, b = a^{-1}$.



(b) Plot of number of 8 cycles as the switch changes for $p = 613, a = 5, b = 2a^{-1}$.



(c) Plot of number of 12 cycles as the switch changes for $p = 613, a = 5, b = 2a^{-1}$.

Figure 7.10

This has solutions $ab = 4$ or $ab = 1 \pmod p$. For $ab = 4 \pmod p$, $\ker(\Omega - I) = 1$ while for $ab = 1 \pmod p$, putting $ab = 1$ into Ω yields the identity matrix and hence $\ker(\Omega - I) = 2$. For parameters satisfying $ab = 1 \pmod p$ we see anomalous distribution as the period distribution has an abundance of 6 cycles following the above word. For example, with $p = 769, a = 5, b = a^{-1} \pmod p = 154, s = 0.5$ we see 5852 six cycles out of the total of 6549 cycles. The parameters satisfying $ab = 4 \pmod p$ correspond to period 2 cycles with word $\omega = ab$. Writing the matrix word explicitly,

$$T_p^2(x, y) = AB(x, y) \pmod p = \begin{bmatrix} ab-1 & -a \\ b & -1 \end{bmatrix} \begin{pmatrix} x \\ y \end{pmatrix} \pmod p = \begin{bmatrix} 3 & -a \\ b & -1 \end{bmatrix} \begin{pmatrix} x \\ y \end{pmatrix} \pmod p. \tag{7.43}$$

Now for period 2 points, we require

$$\begin{bmatrix} 3 & -a \\ b & -1 \end{bmatrix} \begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} x \\ y \end{pmatrix} \pmod p \tag{7.44}$$

which is satisfied when $2x - by = 0 \pmod p$. We will get approximately $p/4$ solutions for this. For example, for $p = 769$, $a = 5$, $b = 4a^{-1} \pmod p = 616$ we have 192 distinct orbits of period 2. Note that 192*4 = 768.

Also for $w = bbabaaba$ and with corresponding word matrix $\Omega = BBABAABA$ we have

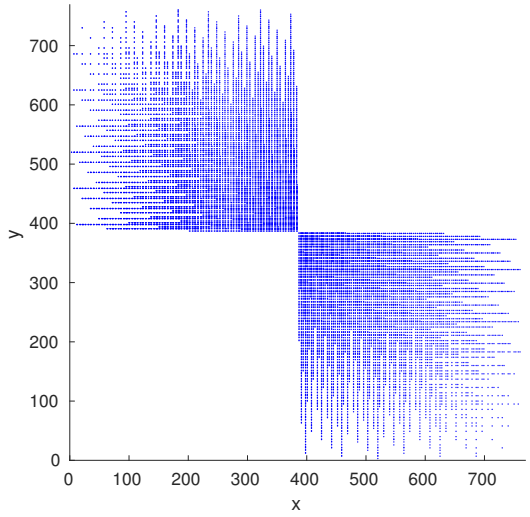
$$\text{trace}(\Omega) - 2 = (ab + a + b)(ab - a - b)(ab - 2)^2 \tag{7.45}$$

and for $ab = 2 \pmod p$ we again get the identity matrix for Ω. Figure 7.11b shows the points with period 8 for $p = 613, a = 117, b = 2a^{-1}, s = 0.5$. Note that for parameters satisfying $ab - a - b = 0$ we obtain 4 cycles with word $BAAB$. For $w = bababaababab$ with corresponding word matrix $\Omega = BABABAABABAB$ we have

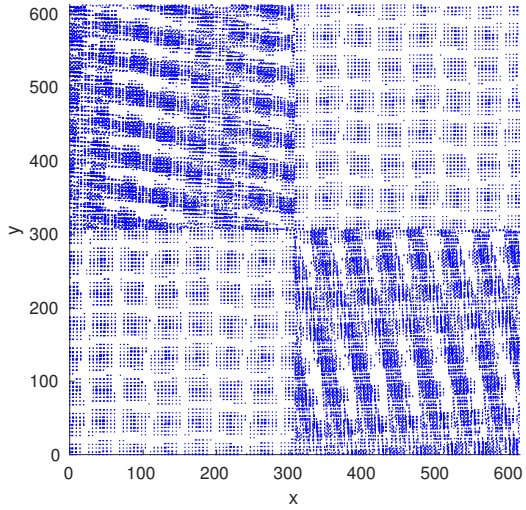
$$\text{trace}(\Omega) - 2 = (ab + a + b)(ab - a - b)(ab - 1)^2(ab - 3)^2 \tag{7.46}$$

and for $ab = 3 \pmod p$ we see the identity matrix for Ω. Figure 7.11c shows the points with period 8 for $p = 769, a = 41, b = 3a^{-1}, s = 0.5$.

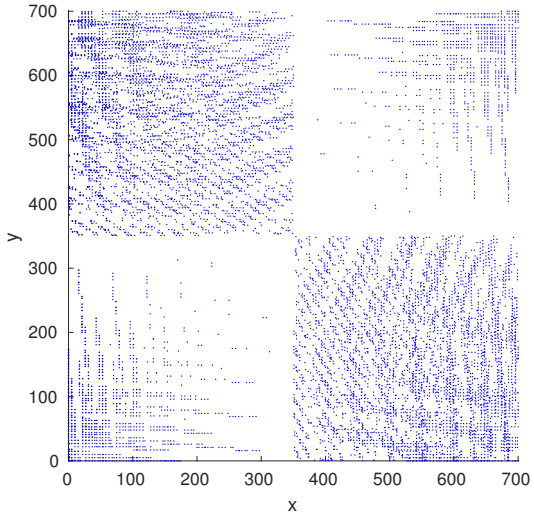
The anomalous values of these above parameter values can be seen in figure 7.9 where we have rescaled the x axis to be $1/a \pmod p$. For $s = 0.5$ we provide plots illustrating the proportion of space taken up by the singular codes corresponding to the parameter



(a) Plot of period 6 points for $p = 769, a = 542, b = a^{-1}$ showing a very distinct pattern.



(b) Plot of period 8 points for $p = 613, a = 117, b = 2a^{-1}$ showing a very distinct pattern.



(c) Plot of period 12 points for $p = 769, a = 542, b = 3a^{-1}$ showing a very distinct pattern.

Figure 7.11: Plot showing period $6, 8, 12$ points for parameters satisfying $ab = 1, 2, 3$ respectively corresponding to words $\omega = ababab, aababbab, bababaababa$.

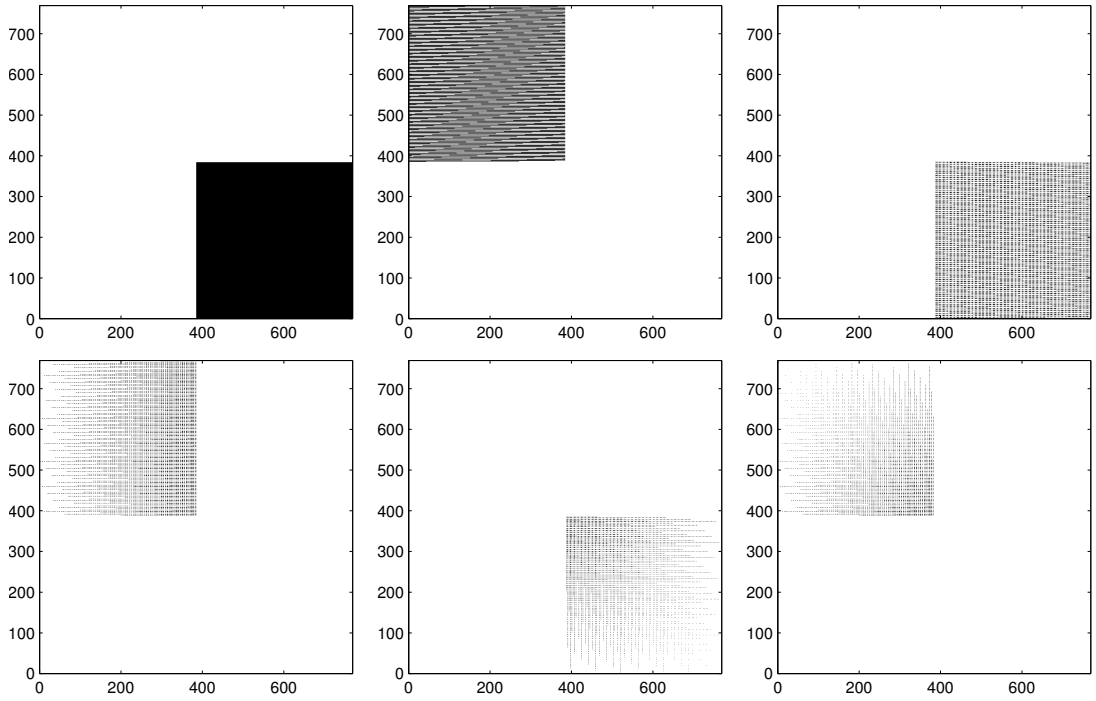
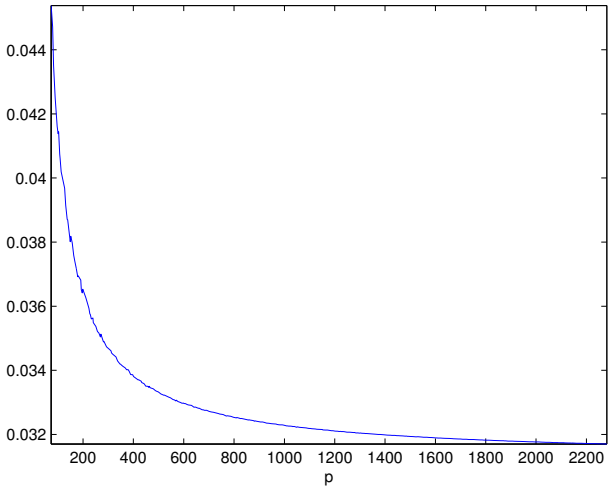


Figure 7.12: Plot of filtering at each stage for 6 cycles.

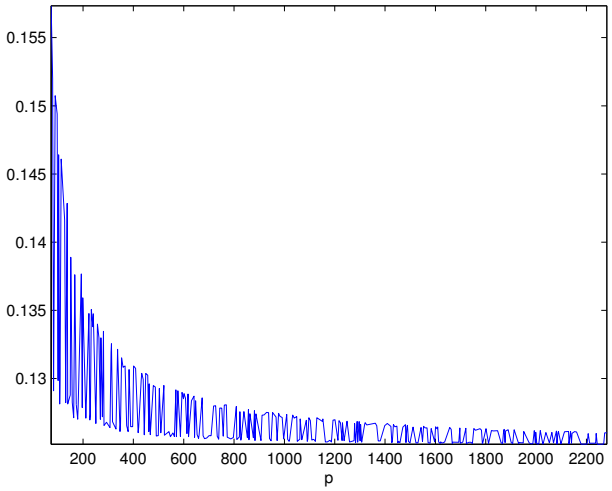
values $ab = 1, 2, 3 \pmod{p}$ in figure 7.13a 7.13b 7.13c. As $p \to \infty$ the proportion seems to converge to a non-zero limit.

Claim 7.4.2. The average proportion of the integer lattice taken up by period 6 orbits for parameters satisfying $ab = 1$ ($s = 0.5$) is $1/32$ or 3.125% as $p \to \infty$.

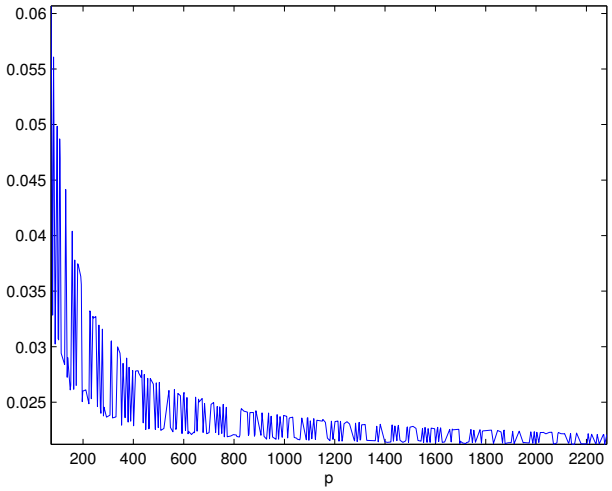
Remark 7.4.3. Consider the action of the map B on the left half of the torus. This will map it to another quadrilateral with the same area but sheared. If we look on the unit square, it will look like it has been sliced into many pieces which approximately distribute it evenly with respect to the number of points with x coordinate less than $s = 0.5$ and greater than $s = 0.5$. In other words, heuristically we can think that there is a 50% chance of applying either map A or B at each iteration. So given a point (x, y), the x coordinate will determine which map is applied first. Then for each subsequent mapping there is a 50% chance of alternating which we must do 5 times. Thus yielding the value $1/32$ or 3.125%. This is shown in figure 7.12 where the top left is the image of the mapping of the left half of the unit square and subsequent plots show the filtering out of points that do not follow the word $BABABA$. Figure 7.13a shows the average proportion of the integer lattice taken up by period 6 orbits for parameters satisfying $ab = 1$ seems to approach this value. Figure 7.11c shows all the period 6 points with word $ABABAB$ or $BABABA$ for $p = 769, a = 542, b = a^{-1}$.



(a) The average proportion of the integer lattice taken up by period 6 orbits over all parameters (b^{-1}, b) for all primes from $p = 73$ to $p = 2281$ and $s = 0.5$.



(b) The average proportion of the integer lattice taken up by period 8 orbits over all parameters $(2b^{-1}, b)$ for all primes from $p = 73$ to $p = 2281$ for $s = 0.5$.



(c) The average proportion of the integer lattice taken up by period 12 orbits over all parameters $(3b^{-1}, b)$ for all primes from $p = 73$ to $p = 2281$ for $s = 0.5$.

Figure 7.13

Now suppose we are interested in a particular word ω. We are interested which parameters a, b, s, p we observe this ω in the dynamics. From above, we know that a necessary condition is that

$$C = \text{trace}(\Omega) - 2 = 0 \pmod{p}. \tag{7.47}$$

This is an equation in a, b and it is known that it can be expressed as a polynomial with variables $(tr(A), tr(B), tr(AB))$ [56, 34]. For a unimodular matrix A, applying the Cayley-Hamilton theorem, we get

$$A^2 = \alpha A - I \tag{7.48}$$

where $\alpha = \text{trace}(A)$ and I is the identity matrix. By repeatedly applying this equation, we can represent the kth matrix power of A in terms of (the 1st power of) A using the following recursive formula:

$$A^k = d_k(\alpha)A - d_{k-1}(\alpha)I, \tag{7.49}$$

where $d_k(\alpha)$ is a polynomial in α such that

$$d_{k+1}(\alpha) = \alpha d_k(\alpha) - d_{k-1}(\alpha), \tag{7.50}$$

$$d_1(x) = 1 \tag{7.51}$$

$$d_0(x) = 0. \tag{7.52}$$

Let B also be a unimodular matrix with $\text{trace}(B) = \beta$. Then using equation (7.49) for A and B,

$$\begin{aligned}\text{trace}(A^k B^l) &= \text{trace}((d_k(\alpha)A - d_{k-1}(\alpha)I)(d_l(\beta)B - d_{l-1}(\beta)I)) \\ &= d_k(\alpha)d_l(\beta)\,\text{trace}(AB) - \alpha d_k(\alpha)d_{l-1}(\beta) - \beta d_{k-1}(\alpha)d_l(\beta) + 2d_{k-1}(\alpha)d_{l-1}(\beta).\end{aligned} \tag{7.53}$$

Now let s_1, s_2 be arbitrary unimodular matrices (such as products of unimodular matrices A, B). Using equation (7.53) with $B = s_2 s_1$ and $l = 1$ and noting that trace is invariant under cyclic permutation,

$$\text{trace}(s_1 A^k s_2) = d_k(\alpha)\,\text{trace}(s_1 A s_2) - 2d_{k-1}(\alpha)\,\text{trace}(s_1 s_2). \tag{7.54}$$

Using equation (7.49), (7.53), (7.54) we can represent the trace of any product of matrix powers in A and B as a polynomial function of $(tr(A), tr(B), tr(AB))$.

For our case, $\text{trace}(A) = a, \text{trace}(B) = b, \text{trace}(AB) = ab - 2$. So C will be polynomial in a, b of degree length of ω. The Hasse-Weil bound states that for a irreducible curve C in a finite field with characteristic p, we have

$$|\#C - (p+1)| \leq 2g\sqrt{p} \tag{7.55}$$

where $\#C$ is the number of solutions and g is the genus of C. The genus of an irreducible curve C is $g \leq (d-1)(d-2)/2$ where d is the degree of C with equality if C has no singularities. Each singularity reduces the genus depending on its multiplicity. This will give us a bound on the maximum number of parameter values for each p where we see particular words.

We may systematically classify words into parameters which they can occur in. Note that trace of a product is invariant under cyclic permutation. (Also without loss of generality we can look at words with $\#a \geq \#b$.) The valid parameter values are obtained using the trace condition where we have also excluded smaller factors (e.g. the condition for $\omega = a$ is not included in $\omega = aa$). Table 7.1 shows all the words of length 1 to 5 and the corresponding parameter values a, b where they can occur.

Recall that in the heat map 7.5, we saw vertical (horizontal) lines which correspond the words ω consisting of just one letter a (or b). By explicitly solving the trace equation for ω with repeated a we can find the potential positions of these lines. For example, consider the word $\omega = aaaaa$. We see this when a satisfies

$$a^2 + a - 1 = 0 \pmod{p}. \tag{7.56}$$

From section 6.3 we know that if $s = 0$ all points have the same period length. For non-zero s, we approximate the proportion taken up by these 5 cycles by $(1-s)^5$. So, even for $s = 0.5$, we expect to see $1/32$ of the phase space consumed by cycles of length 5. Now for a given p, the solutions to (7.56) are

$$a = \frac{-1 \pm \sqrt{5}}{2} \pmod{p}. \tag{7.57}$$

Table 7.1: Classification of all possible words for period 1 to 5 with the corresponding a, b where they can occur. All equations here are read modulo p.

t	ω	a, b
1	a	$a = 2$
2	aa	$a = -2$
	ab	$ab = 4$
3	aaa	$a = -1$
	aab	$(a+1)(ab-b-2) = 0$
4	$aaaa$	$a = 0$
	$aaab$	$a(a^2 - 2a - 2b) = 0$
	$abab$	$ab = 0$
	$aabb$	$(ab+a+b)(ab-a-b) = 0$
5	$aaaaa$	$a^2 + a - 1 = 0$
	$aaaab$	$(a^2+a-1)(a^2-ab-2a-b+2) = 0$
	$aaabb$	$(ab+a-1)(a^2b-a^2-a-2b+2) = 0$
	$aabab$	$(ab+b-1)(a^2-ab-3a+2) = 0$
6	$aaaaaa$	$a = 1$
	$aaaaab$	$(a-1)(a+1)(a^3b-2a^2-3ab+4) = 0$
	$aaaabb$	$(a^2b+a^2+ab-b-2)(a^2b-a^2-ab-b+2) = 0$
	$aaabab$	$(ab-1)(a^3b-3a^2-2ab+4) = 0$
	$aabaab$	$(a-1)(a+1)(ab+b-2)(ab-b-2) = 0$
	$aaabbb$	$(ab-1)(a^2b^2-2a^2-ab-2b^2+4) = 0$
	$aababb$	$a^3b^3-a^3b-4a^2b^2-ab^3+2a^2+5ab+2b^2-4 = 0$
	$ababab$	$ab = 1$

We have 5 as a quadratic residue if and only if $p = \pm 1 \pmod 5$. Thus for these primes, we will see vertical lines at the values of a in (7.57). For example, if $p = 769$, we will obtain the solutions $a = 338, 430$ and we see vertical (horizontal) lines for those values in figure 7.5. We will provide the conditions in table 7.2 for these singular words of repeated a for period 6 to 12.

Table 7.2: Classification of period 6 to 12 words with repeated a. All equations here are read modulo p.

t	ω	a
6	$aaaaaa$	$a = 1$
7	$aaaaaaa$	$a^3 + a^2 - 2a - 1 = 0$
8	$aaaaaaaa$	$a^2 - 2 = 0$
9	$aaaaaaaaa$	$a^3 - 3a + 1 = 0$
10	$aaaaaaaaaa$	$a^2 - a - 1 = 0$
11	$aaaaaaaaaaa$	$a^5 + a^4 - 4a^3 - 3a^2 + 3a + 1 = 0$
12	$aaaaaaaaaaaa$	$a^2 - 3 = 0$

We see that the number of solutions to the equations in table 7.2 are consistent with $\phi(t)/2$ from theorem 6.3.9. The equations allow us to find lines of large error. For example, in

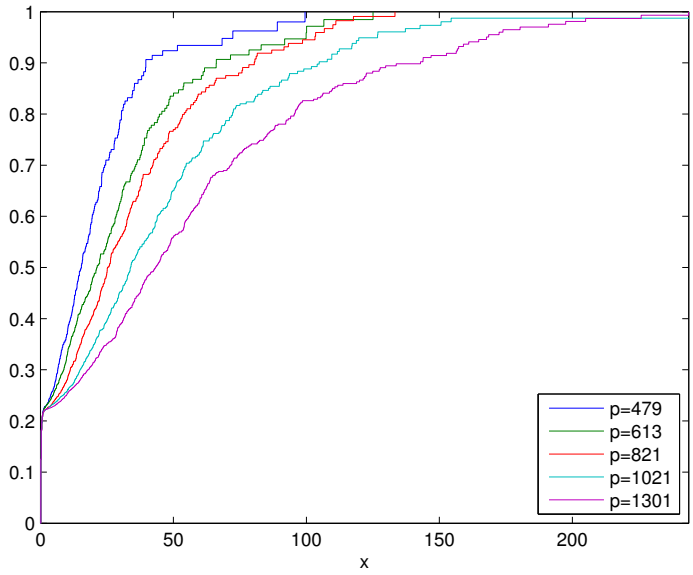


Figure 7.14: Plot of $\mathcal{D}_p(x)$ with parameters $a = 5$ and $b = 2a^{-1}$ for primes $p = 479, 613, 821, 1021, 1301$ showing that the space occupied by small cycles as a proportion of p^2 is constant as p increases.

figure 7.5 we can see distinct lines $a = 2, 311, 338, 430, 594, 632, 768$. From tables 7.1,7.2 we see $a = 2$ corresponds to one cycles $\omega = a$, parameters $a = 768$ correspond to 3 cycles $\omega = aaa$, parameters $a = 338, 430$ correspond to 5 cycles $\omega = aaaaa$, and $a = 311, 594, 632$ correspond the 7 cycles $\omega = aaaaaaa$.

However, the parameter values in tables 7.1,7.2 are not sufficient conditions and a natural question then is if for any given word ω, there exists a, b, p, s such that there exists a point (x, y) under T_p where we see this word. We have found this is not true.

Example 7.4.4. Consider $\Omega = ABABABAB$. This word cannot exist for any a, b, p, s such that $a \neq b$ or $s \neq 0$. We find that $\text{trace}(ABABABAB - I) = ab(ab-4)(ab-2)^2$. The first 2 factors correspond to period 4 and 2 words respectively. For $ab = 2$ we find that $ABAB = -Id$. So $ABAB(x, y) = (-x, -y)$, but this ensures this is an unallowable word.

7.5 Concluding Remarks

In this chapter, we studied a three-parameter family of piecewise linear maps. We studied the distribution of the length of its orbits, seeing a departure from the singular distribution of the linear map to $\mathcal{R}(x)$, the gamma distribution with with shape parameter 2 and scale parameter 1. We also observed that anomalous parameter values where we see many

repeated orbits of the same length, something we do not expect to see for polynomial automorphisms whose limiting distribution of orbit lengths is also $\mathcal{R}(x)$. This comes from the piecewise linear nature of map where we may still see remnants of the linear action of the map. However, the proportion of these parameter pairs seems to vanish and this was stated in conjecture 7.3.1. Thus, although we can see that the individual details of the map can be useful in eliciting its behaviour, the asymptotic behaviour is still largely governed by its reversibility property as seen in the asymptotic distribution of orbit lengths.

Chapter 8

Reversible birational maps over finite fields

In this chapter, we consider reversible birational maps with no integrals. We will revise previous results on the orbit statistics of these maps in 2D without integrals and a probabilistic model to find the expected statistics of these reversible maps [64]. In 2005, Roberts and Vivaldi conjectured that the distribution of period lengths for reversible maps in the limit was $\mathcal{R}(x)$. In 2009 [64], they used a combinatorial model that showed that the expected distribution for the composition of two involutions was $\mathcal{R}(x)$. Here the number of fixed points of each of the involutions was fixed. Lugo [43] has also studied the cycle structure of compositions of random involutions with no restrictions, and those with no fixed points. It should be noted that the composition of two involutions is a permutation but that sampling this uniformly at random is not the same as picking a random permutation. Burnette and Schmutz [10] studied the number of ways of representing random permutations as a composition of two involutions and showed that for large n, most permutations $\sigma \in S_n$, the number of representations of σ by ordered pairs of involutions $\mathbf{N}_n(\sigma)$ is

$$e^{(\frac{1}{2}-\epsilon)\log^2 n} < \mathbf{N}_n(\sigma) < e^{(\frac{1}{2}+\epsilon)\log^2 n}. \tag{8.1}$$

For non-reversible maps, we saw that the statistics of random permutations could be used to model the number of cycles in chapter 3 and 4. For reversible maps, we extend the probabilistic model by Roberts and Vivaldi [64] to account for singular orbits and find average statistics for their orbit lengths. We observe that the expected distribution of cycles in the composition of two involutions is (asymptotically) $\mathcal{R}(x)$ which is universal when appropriately scaled. This was conjectured for the distribution of reversible polynomial automorphisms by the same authors in 2005 [63]. We will also see this distribution

for birational maps. Here, we put a larger focus on the asymmetric periodic orbits, in particular in their expected number which was not previously considered. We will see the usefulness of this statistic in detecting the number of integrals in reversible maps in chapter 9.

We extend the model in [64] to allow for singular points to represent those in reversible birational maps on the space $\mathbb{F}_p^d$. This also accounts for the case with no singularities. Now the involutions G, H will have domains a subset of N. They satisfy the involutory property $G^2 = I$ and $H^2 = I$ where defined. The set of points where they are not defined are called singular sets, denoted by $\mathrm{Sing}(G)$ and $\mathrm{Sing}(H)$ respectively. Then the singular sets for L and L^{-1} are given by

$$\mathrm{Sing}(L) = \mathrm{Sing}(H \circ G) = \mathrm{Sing}(G) \cup G(\mathrm{Sing}(H)), \tag{8.2}$$

$$\mathrm{Sing}(L^{-1}) = \mathrm{Sing}(G \circ H) = \mathrm{Sing}(H) \cup H(\mathrm{Sing}(G)). \tag{8.3}$$

Now we obtain four types of orbits depending on whether they intersect the fixed sets and the singular sets or not, namely

1. symper symmetric periodic orbits,
2. asymper asymmetric periodic orbits,
3. asymaper asymmetric aperiodic orbits,
4. symaper symmetric aperiodic orbits.

Symmetric periodic orbits contain two points of the sets $\mathrm{Fix}(G)$ and $\mathrm{Fix}(H)$ while symmetric aperiodic orbits contain only one point. Let $g = \#\mathrm{Fix}(G)$ and $h = \#\mathrm{Fix}(H)$. This gives us the equation

$$2\#symper + \#symaper = g + h. \tag{8.4}$$

Also let $\gamma = \#\,\mathrm{Sing}(G)$ and $\eta = \#\,\mathrm{Sing}(H)$. Aperiodic orbits must reach one point $\mathrm{Sing}(L)$ in forward time and one point in $\mathrm{Sing}(L^{-1})$ in backward time. Then we obtain

$$\#symaper + \#asymaper = \gamma + \eta. \tag{8.5}$$

These two equations constrain the number of symmetric periodic, symmetric aperiodic and asymmetric aperiodic orbits. The asymmetric periodic orbits are not constrained

directly by g, h, γ, η, and it is possible that they do not exist at all. The combinatorial model will be used to count the expected number of these orbits. In essence, by using this model, we are saying that the dynamics of a reversible map is controlled mainly by its number of fixed points and singular points and not necessarily in the particular details of the map.

8.1 Combinatorial model

In [64], one of the the main focuses was using the combinatorial model to obtain the expected distribution of the cycle lengths in the reduction to the finite space $\mathbb{F}_p^d$. It was shown that the expected orbit distribution for the composition of two involutions was $\mathcal{R}(x)$ and that the proportion of asymmetric periodic points was asymptotically zero. A similar idea was used in chapter 4 to model birational maps. Here, we extend the model to provide the expected number of asymmetric cycles and also allow for singularities. Although in most cases, the proportion of points belonging to asymmetric cycles is small and in the limit approaches zero, the expected number of asymmetric cycles is non-zero. By counting the numbers of each type of orbit, we can find the asymptotic expected values for their distribution, the number of each type of orbit, and the number of points corresponding to each type of orbit. The calculations for each are similar as we count the number of k-orbits for each type, sum over k and take the asymptotic limit. The main ingredients for counting the statistics of the orbits is by considering the number of ways of building each type of orbit in terms of the reduction in size of fixed sets and singular sets and of the phase space. We also account for the reversibility property of the symmetric orbits which have symmetry about the fixed sets of G and H and asymmetric orbits which come in pairs.

It was shown that the combinatorial model produced the same distribution as observed in reversible polynomial automorphisms. For birational maps with the reversibility property, we also need to account for the involutions having singular points. Orbits reaching these points will be not be periodic, and we expect different statistics for the periodic orbits. In addition, these singular orbits may also consume points in the fixed sets, and hence the number of symmetric orbits in general will be less than $(g + h)/2$. By incorporating singular points into the involutions of the model, we are able to model various statistics of the composition of random involutions with singularities. We provide evidence that these statistics model reversible birational maps well.

8.1.1 Composition of random involutions

Let N be a positive integer. Let $0 \leq g, h, \gamma, \eta \leq N$ such that $N-(g+\gamma)$ and $N-(h+\eta)$ are both even. We consider ordered pairs (G, H) of random involutions on a set of $N-\gamma$ and $N-\eta$ points respectively. In addition, G and H fix g, h points respectively, so G has $(N-g-\gamma)/2$ two-cycles and similarly H has $(N-h-\eta)/2$. For each pair (G, H) we consider the composition $L = H \circ G$. This will decompose into four types of orbits described previously. We are interested in various statistics corresponding to these orbits. Consider the space of the composition of two involutions G, H on N points.

Lemma 8.1.1. *Let $\mathbf{E}(g, h, \gamma, \eta, N)$ be the set of all involutions with the given parameters. Then the number of such pairs of involutions is given by*

$$\#\mathbf{E}(g, h, \gamma, \eta, N) = \frac{1}{2^{N-(g+h+\gamma+\eta)/2}} \frac{(N!)^2}{g!h!\gamma!\eta![(N-g-\gamma)/2]![(N-h-\gamma)/2]!}. \tag{8.6}$$

Proof. The number of involutions G on N points with g fixed points and γ singular points is given by

$$\binom{N}{g}\binom{N-g}{\gamma} \frac{(N-g-\gamma)!}{2^{(N-(g+\gamma)/2)}[(N-g-\gamma)/2]!} \tag{8.7}$$

where the first term is the number of ways of choosing g fixed points, the second term is the number of ways of choosing γ singular points, and the third term is the number of ways of partitioning the remaining points into two-cycles. Multiplying this with the corresponding expression for the number of involutions H on N points with h fixed and η singular points, we obtain the required number. □

Our methodology is as follows. For each type of orbit, we count the number of possible orbits of length k. From this, it is possible to obtain the number of points belonging to orbits of the length k and hence also the distribution by summing and scaling appropriately. The inclusion of singularities yields additional points in the phase space where we must avoid in the construction of asymmetric periodic orbits. In a sense, they play a similar role to the fixed sets of the involutions. If an orbit reaches a singular point in forward time, it must also reach a singular point in backward time in which case, the singular orbit is completed. A singular orbit may also be symmetric if it intersects either of the fixed sets. It can only hit at most one. (If an orbit hits two symmetric points, then is necessarily a symmetric periodic orbit.) We are interested in the expected values for L with the specified parameters. For fixed N, our phase space is finite and we can provide

exact calculations for the expected values for the various statistics involving sums and products. However, for more meaningful results we provide asymptotic analysis yielding computationally efficient and relatively accurate results. Let us define

$$z = g + h + \gamma + \eta \tag{8.8}$$

as this term will appear frequently. We summarise the results below. In the following, by asymptotic results (unless otherwise stated), we mean that as

$$N \to \infty, \qquad \frac{z}{N} \to 0. \tag{8.9}$$

Theorem 8.1.2. *The asymptotic expected number of the four types of orbits is given by*

$$\langle \#symper \rangle = \frac{1}{2}\frac{(g+h)^2}{z} \tag{8.10}$$

$$\langle \#symaper \rangle = \frac{(g+h)(\gamma+\eta)}{z} \tag{8.11}$$

$$\langle \#asymaper \rangle = \frac{(\gamma+\eta)^2}{z} \tag{8.12}$$

$$\langle \#asymper \rangle = \log\left(\frac{N}{z}\right). \tag{8.13}$$

Corollary 8.1.3. *The expected number of orbits (of all types) asymptotically is*

$$\#\sigma = \frac{z}{2} + \frac{(\gamma+\eta)^2}{2z} + \log\left(\frac{N}{z}\right). \tag{8.14}$$

These expected values satisfy (8.4) and (8.5). Also if $\gamma = \eta = 0$, then there are no aperiodic orbits and the number of symmetric periodic orbits is

$$\frac{g+h}{2} \tag{8.15}$$

as expected for a reversible map with no singularities.

Theorem 8.1.4. *The asymptotic distribution of the four types of orbits with scaling factor* $\kappa = \frac{N}{g+h+\gamma+\eta}$ *is given by*

$$\mathcal{R}^{symper}(x) \sim \frac{(g+h)^2}{z^2}\mathcal{R}(x) \tag{8.16}$$

$$\mathcal{R}^{symaper}(x) \sim \frac{2(g+h)(\gamma+\eta)}{z^2}\mathcal{R}(x) \tag{8.17}$$

$$\mathcal{R}^{asymaper}(x) \sim \frac{(\gamma+\eta)^2}{z^2}\mathcal{R}(x) \tag{8.18}$$

$$\mathcal{R}^{asymper}(x) \sim \frac{1}{z}(1-e^{-x}). \tag{8.19}$$

Corollary 8.1.5. *The asymptotic proportion of space consumed by the four types of orbits is*

$$\langle P^{symper}\rangle = \frac{(g+h)^2}{z^2} \tag{8.20}$$

$$\langle P^{symaper}\rangle = \frac{2(g+h)(\gamma+\eta)}{z^2} \tag{8.21}$$

$$\langle P^{asymaper}\rangle = \frac{(\gamma+\eta)^2}{z^2} \tag{8.22}$$

$$\langle P^{asymper}\rangle = \frac{1}{z}. \tag{8.23}$$

Corollary 8.1.6. *The asymptotic number of points in the four types of orbits is*

$$\langle \#symperpt\rangle = \frac{N(g+h)^2}{z^2} \tag{8.24}$$

$$\langle \#symaperpt\rangle = \frac{2N(g+h)(\gamma+\eta)}{z^2} \tag{8.25}$$

$$\langle \#asymaperpt\rangle = \frac{N(\gamma+\eta)^2}{z^2} \tag{8.26}$$

$$\langle \#asymperpt\rangle = \frac{N}{z}. \tag{8.27}$$

The sum of the first three distributions in theorem 8.1.4 is $\mathcal{R}(x)$ and their coefficients give the fraction of space occupied by orbits of their respective type. The asymmetric periodic orbits have asymptotically zero density which can be seen by the coefficient of $(1-e^{-x})$. To obtain the asymptotic number of points of each type given in corollary 8.1.6, we simply multiply the proportions in corollary 8.1.5 by N.

8.1.2 Number and bounds on asymmetric periodic points and cycles

Theorem 8.1.7 states the expected number of asymmetric cycles (and points) of each length k and by summing we also obtain the total expected number of asymmetric cycles (and points).

Theorem 8.1.7. *Let $L = H \circ G$ be the composition of two involutions on a space with N points. Denote $g(N), h(N)$ as the size of the fixed sets of G, H and $\gamma(N), \eta(N)$ as the size of the singular sets of G, H. The expected number of asymmetric periodic points and asymmetric periodic cycles of length k is:*

$$\langle \#asymper_k \rangle = \frac{1}{k} \prod_{j=0}^{k-1} \left(1 - \frac{g+\gamma-1}{N-(2j+1)}\right)\left(1 - \frac{h+\eta}{N-2j}\right) \tag{8.28}$$

$$\langle \#asyperpt_k \rangle = k\langle \#asymper_k \rangle \tag{8.29}$$

and it follows by summing over k we can obtain the expected number of asymmetric periodic points and asymmetric periodic cycles,

$$\langle \#asymper \rangle = \sum_{k=1}^{kmax} \frac{1}{k} \prod_{j=0}^{k-1} \left(1 - \frac{g+\gamma-1}{N-(2j+1)}\right)\left(1 - \frac{h+\eta}{N-2j}\right) \tag{8.30}$$

$$\langle \#asymperpt \rangle = \sum_{k=1}^{kmax} \langle \#asymperpt_k \rangle = \sum_{k=1}^{kmax} k\langle \#asymperpt_k \rangle \tag{8.31}$$

where $kmax = \frac{N-\max(g,h)-\max(\gamma,\eta)}{2}$ is the maximum length of an asymmetric periodic orbit.

The value for $kmax$ is obtained by noting that asymmetric periodic cycles must come in pairs and can't occupy any of the points in the fixed sets or singular sets of G and H. The result on the expected number of asymmetric orbits is the most important result in this chapter. This was not studied in [64] and it will prove useful as a discriminator for the number of integrals in a reversible map in chapter 9. Thus, we put most of the detail in this proof, and provide a sketch of the proof for some of the other statistics following. However, the method for counting any type of orbit is largely the same as in [64] with some modifications needed to adjust for the different types of orbits. We now derive the result for the number of asymmetric periodic orbits and points.

Proof. (Theorem 8.29) We count all possible asymmetric k-cycles in the $\mathbf{E}(g,h,\gamma,\eta,N)$ pairs of involutions, and divide by the number of pairs of involutions $\mathbf{E}(g,h,\gamma,\eta,N)$ to obtain the expected value. Now, asymmetric k-cycles come in pairs, mapped to one another under G. We relate this pair to a periodic $2k$-arc connecting a point $x_1 \in \Omega$ that is not in $\mathrm{Fix}(G)$ or $\mathrm{Fix}(H)$ to itself:

$$(x_1, y_1, \ldots, x_k, y_k) \quad y_j = G(x_j) \neq x_j, \;\; x_{j+1} = H(y_j) \neq y_j \pmod{k}, \quad j = 1, \ldots, k \geq 1. \tag{8.32}$$

We compute the expected number of asymmetric cycles of length k. Let us fix a specific arc Γ of the form (8.32), corresponding to two explicit cycles of length k. Consider looking for this pair across the ensemble $\mathbf{E}(g,h,\gamma,\eta,N)$, using the indicator function $\mathbf{1}_\Gamma$ which is 1 if Γ is present in an element of the ensemble and 0 otherwise. Then the expected number of appearances of the arc Γ is given by $\langle \#_\Gamma \rangle = (\sum_{\mathbf{E}} \mathbf{1}_\Gamma)/\#\mathbf{E}(g,h,\gamma,\eta,N) = \#\mathbf{E}(g,h,\gamma,\eta,N-2k)/\#\mathbf{E}(g,h,\gamma,\eta,N)$, where the numerator of the latter is the number of ensemble members that contain Γ. Note there is no reduction in the cardinalities of the involution fixed sets and their singular sets between numerator and denominator as Γ contains no points of such sets. It remains to count the number of distinct Γ that can be built in the ensemble. Each Γ corresponds to 2 k-cycles and there are $N^{\underline{2k}}$ possible arcs Γ. But we must quotient out from this the number of arcs that correspond to one and the same pair. A cyclic permutation of the $\{x_j, y_j\}$ pairs in Γ (k possibilities) gives the same pair as does the switch $x_j \leftrightarrow y_j$ together with reversing the order of the switched pairs (2 possibilities). So we have:

$$\langle \#asymper_k \rangle = 2\,\frac{N^{\underline{2k}}}{2k}\,\frac{\#\mathbf{E}(g,h,\gamma,\eta,N-2k)}{\#\mathbf{E}(g,h,\gamma,\eta,N)} \tag{8.33}$$

$$= \frac{N^{\underline{2k}}}{k} 2^{2k} \left(\frac{(N-2k)!}{N!}\right)^2 \frac{\left(\frac{N-(g+\gamma)}{2}\right)! \left(\frac{N-(h+\eta)}{2}\right)!}{\left(\frac{N-(g+\gamma)}{2}-k\right)! \left(\frac{N-(h+\eta)}{2}-k\right)!} \tag{8.34}$$

$$= \frac{2^{2k}}{kN^{\underline{2k}}} \left(\frac{N-(g+\gamma)}{2}\right)^{\underline{k}} \left(\frac{N-(h+\eta)}{2}\right)^{\underline{k}} \tag{8.35}$$

$$= \frac{1}{k} \prod_{j=0}^{k-1} \frac{[N-2j-(g+\gamma)]\,[N-2j-(h+\eta)]}{(N-2j)(N-2j-1)} \tag{8.36}$$

$$= \frac{1}{k} \prod_{j=0}^{k-1} \left(1 - \frac{g+\gamma-1}{N-(2j+1)}\right) \left(1 - \frac{h+\eta}{N-2j}\right). \tag{8.37}$$

This is the exact value for the expected number of asymmetric k-cycles. By summing over k, we obtain the expected number of asymmetric cycles as required. □

Unlike the number of cycles for random permutations and s-permutations in chapter 3 and 4 there is no (simple) closed form expression for this sum of products. There are various ways we can approximate it using asymptotic values. We present a conjecture that rewrites the number of asymmetric periodic orbits in (8.30) into an alternate form which can be used to obtain bounds on this number, as well as exact numbers for special parameter values. Note that $N, g+\gamma, h+\eta$ must be of all the same parity.

Conjecture 8.1.8. *The expected number of asymmetric periodic orbits for even $N, g+\gamma, h+\eta$ is*

$$\langle \#asymper \rangle = H_{\frac{N}{2}-\frac{1}{2}} - H_{\frac{z}{2}-\frac{1}{2}} + \sum_{k=1}^{\frac{\min(g+\gamma,h+\eta)}{2}} \frac{1}{k} \prod_{j=0}^{k-1} \frac{(g+\gamma-2j)(h+\eta-2j)}{(N-2j)(z-2j-1)} \tag{8.38}$$

and for odd $N, g+\gamma, h+\eta$ is

$$\langle \#asymper \rangle = H_{\frac{N+1}{2}-\frac{1}{2}} - H_{\frac{z}{2}-\frac{1}{2}} + \sum_{k=1}^{\frac{\min(g+\gamma,h+\eta)-1}{2}} \frac{1}{k} \prod_{j=0}^{k-1} \frac{(g+\gamma-2j-1)(h+\eta-2j-1)}{(N-2j-1)(z-2j-1)}. \tag{8.39}$$

Although the above form still contains a sum of products as in (8.30), notice that asymptotically, this sum of products vanishes. Also notice the appearance of the harmonic numbers again which hints at some similarity to the results in earlier chapters. The form written above using harmonic numbers with half integers is more for convenience of notation as the difference of these two half integer valued harmonic numbers can be written in terms of integer valued harmonic numbers. This is shown in the following lemma which is straightforward to prove.

Lemma 8.1.9. *For non-negative integers a, b, we have*

$$H_{b-\frac{1}{2}} - H_{a-\frac{1}{2}} = \sum_{j=a}^{b-1} \frac{1}{j+\frac{1}{2}} = 2H_{2b-1} - H_{b-1} - (2H_{2a} - H_a). \tag{8.40}$$

If $g+\gamma = 0$ or $h+\eta = 0$ we can obtain a simple exact value for the number of asymmetric periodic orbits by using the above conjecture in terms of Harmonic numbers.

Corollary 8.1.10. *Suppose that $g+\gamma = 0$. Then, necessarily, $h+\eta, N$ are also even. Then the number of asymmetric periodic orbits is*

$$\langle \#asymper \rangle = H_{\frac{N}{2}-\frac{1}{2}} - H_{\frac{h+\eta}{2}-\frac{1}{2}} = \sum_{j=(h+\eta)/2}^{N/2-1} \frac{1}{j+\frac{1}{2}}. \tag{8.41}$$

In particular, if $g+\gamma = 0 = h+\eta$, then the number of asymmetric periodic orbits is

$$\langle \#asymper \rangle = H_{\frac{N}{2}-\frac{1}{2}} - H_{-\frac{1}{2}} = \sum_{j=0}^{N/2-1} \frac{1}{j+\frac{1}{2}}. \tag{8.42}$$

This result is similar to the expected number of periodic orbits in an s-permutation in chapter 4 and the expected number of periodic orbits in a random permutation in chapter 3 respectively. We bound the sum of products in (8.30) which gives a practical method for approximating this number especially for large parameter values. We first present two lemmas needed to obtain bounds for the inequality.

Lemma 8.1.11. *The Harmonic numbers have the following expansion using the Euler-Maclaurin formula*

$$H_n = \log n + \xi + \frac{1}{2n} - \sum_{k=1}^{\infty} \frac{B_{2k}}{2kn^{2k}} = \log n + \xi + \frac{1}{2n} - \frac{1}{12n^2} + \frac{1}{120n^4} - \dots \tag{8.43}$$

where B_k are the Bernoulli numbers.

Lemma 8.1.12. *(Convergence of Maclaurin series) Let $S_m = \sum_{n=1}^{m} \frac{x^n}{n}$. Then for $-1 < x < 1$,*

$$\lim_{m\to\infty} S_m = -\log(1-x). \tag{8.44}$$

It is well known that the following identity holds for $|x| < 1$ using Taylor series

$$-\log(1-x) = \sum_{j=1}^{\infty} \frac{x^j}{j}. \tag{8.45}$$

Define the remainder $R_k(x)$ to be

$$R_k(x) = -\log(1-x) - \sum_{j=1}^{k} \frac{x^j}{j}. \tag{8.46}$$

Let $f(x) = -\log(1-x)$. The Cauchy form of the remainder tells us that

$$R_k(x) = \frac{f^{(k+1)}(\xi)}{k!}(x-\xi)^k x \tag{8.47}$$

for some real number ξ between 0 and x. Since $f^k(x) = \frac{(k-1)!}{(1-x)^k}$ for $k \geq 1$, we get

$$R_k(x) = \frac{x}{1-\xi}\left(\frac{x-\xi}{1-\xi}\right)^k. \tag{8.48}$$

For $0 < x < 1$ and $k > x/(1-x)$, we find that $R_k(x) < x^{k+1}$ using elementary calculus and hence

$$|-\log(1-x) - \sum_{j=1}^{k}\frac{x^j}{j}| < x^{k+1}. \tag{8.49}$$

Theorem 8.1.13. *Subject to conjecture 8.1.8, we have the following inequality for all* N, g, h, γ, η

$$H_{\frac{N}{2}-\frac{1}{2}} - H_{\frac{z}{2}-\frac{1}{2}} < \langle \#asymper \rangle < \log\left[\frac{N(N-1)}{N(z-1)-(g+\gamma)(h+\eta)}\right]. \tag{8.50}$$

Proof. The left hand side of the inequality follows directly from conjecture 8.1.8 since each term in the sum of products is positive. Now we consider the right hand side. Using equation (8.30), we have

$$\begin{aligned}
\langle \#asymper \rangle &= \sum_{k=1}^{kmax}\frac{1}{k}\prod_{j=0}^{k-1}\left(1-\frac{g+\gamma-1}{N-(2j+1)}\right)\left(1-\frac{h+\eta}{N-2j}\right) && (8.51)\\
&\leq \sum_{k=1}^{kmax}\frac{1}{k}\prod_{j=0}^{k-1}\left(1-\frac{g+\gamma-1}{N-1}\right)\left(1-\frac{h+\eta}{N}\right) && (8.52)\\
&= \sum_{k=1}^{kmax}\frac{\left[\left(1-\frac{g+\gamma-1}{N-1}\right)\left(1-\frac{h+\eta}{N}\right)\right]^k}{k} && (8.53)\\
&< \sum_{k=1}^{\infty}\frac{\left[\left(1-\frac{g+\gamma-1}{N-1}\right)\left(1-\frac{h+\eta}{N}\right)\right]^k}{k} && (8.54)\\
&= -\log\left[1-\left(1-\frac{g+\gamma-1}{N-1}\right)\left(1-\frac{h+\eta}{N}\right)\right] && (8.55)\\
&= \log\left[\frac{N(N-1)}{N(z-1)-(g+\gamma)(h+\eta)}\right] && (8.56)
\end{aligned}$$

where we have used lemma 8.1.12 for the infinite sum. □

Corollary 8.1.14. *For $N \to \infty$ and $z \to \infty$, we have*

$$\log\left(\frac{N-1}{z}\right) < \langle \#asymper \rangle < \log\left(\frac{N-1}{z-1-\psi}\right) \tag{8.57}$$

where $\psi = \frac{(g+\gamma)(h+\eta)}{N}$.

Proof. We first consider the left inequality. From the left inequality in theorem 8.1.13 we have $H_{\frac{N}{2}-\frac{1}{2}} - H_{\frac{z}{2}-\frac{1}{2}} < \langle \#asymper \rangle$. Now using lemma 8.1.9 and 8.43,

$$\begin{aligned}
&H_{\frac{N}{2}-\frac{1}{2}} - H_{\frac{z}{2}-\frac{1}{2}} \\
&= 2H_{N-1} - H_{\frac{N}{2}-1} - (2H_{z-\frac{1}{2}} - H_{\frac{z}{2}}) \\
&> 2\left[\log(N-1) + \xi + \frac{1}{2(N-1)} - \frac{1}{12(N-1)^2}\right] - \left[\log\left(\frac{N}{2}-1\right) + \xi + \frac{1}{N-2}\right] \\
&\quad - 2\left[\log\left(z-\frac{1}{2}\right) + \xi + \frac{1}{2z-1}\right] + \left[\log\left(\frac{z}{2}\right) + \xi + \frac{1}{z} - \frac{1}{3z^2}\right] \\
&= 2\log(N-1) - \log(N-2) + \log 2 + \frac{1}{N-1} - \frac{1}{N-2} - \frac{1}{6(N-1)^2} \\
&\quad - 2\log\left(z-\frac{1}{2}\right) + \log z - \log 2 - \frac{1}{z-2} + \frac{1}{z} - \frac{1}{3z^2} \\
&> \log(N-1) - \log z + 1 + \frac{1}{N-1} - \frac{1}{N-2} - \frac{1}{6(N-1)^2} - \frac{1}{z-2} + \frac{1}{z} - \frac{1}{3z^2} \\
&> \log(N-1) - \log z
\end{aligned}$$

which is valid for $N, z \geq 4$.

Now for the right inequality, we take the right inequality in theorem 8.1.13 and notice that

$$\log\left[\frac{N(N-1)}{N(z-1)-(g+\gamma)(h+\eta)}\right] = \log\left[\frac{N-1}{z-1-(g+\gamma)(h+\eta)/N}\right] \tag{8.58}$$

which gives the result as required. □

Note that $\psi < \min(g+\gamma, h+\eta) < z$ and asymptotically $\psi = o(z)$.

Corollary 8.1.15. *Then asymptotically we have*

$$\langle \#asymper \rangle \to \log\left(\frac{N-1}{z}\right) \to \log\left(\frac{N}{z}\right). \tag{8.59}$$

This follows directly from corollary 8.1.14. Thus we can use this number as an estimate for the number of asymmetric periodic cycles. We provide similar analysis for the number of asymmetric periodic points. From the combinatorial model, the exact number is given by the sum of products,

$$\langle \#asymperpt \rangle = \sum_{k=1}^{kmax} \langle \#asyperpt_k \rangle = \sum_{k=1}^{kmax} \prod_{j=0}^{k-1} \left(1 - \frac{g+\gamma-1}{N-(2j+1)}\right)\left(1 - \frac{h+\eta}{N-2j}\right). \tag{8.60}$$

We present a conjecture similar to that in conjecture 8.1.8 which rewrites this number.

Conjecture 8.1.16. *The expected number of asymmetric periodic points for even $N, g+\gamma, h+\eta$ is*

$$\langle \#asymperpt \rangle = \frac{N-z}{z+1} + \frac{N+1}{z+1} \sum_{k=1}^{\frac{\min(g+\gamma,h+\eta)}{2}} \prod_{j=0}^{k-1} \frac{(g+\gamma-2j)(h+\eta-2j)}{(N-2j)(z-2j-1)} \tag{8.61}$$

and for odd $N, g+\gamma, h+\eta$ is

$$\langle \#asyperpt \rangle = \frac{N+1-z}{z+1} + \frac{N+2}{z+1} \sum_{k=1}^{\frac{\min(g+\gamma,h+\eta)-1}{2}} \prod_{j=0}^{k-1} \frac{(g+\gamma-2j-1)(h+\eta-2j-1)}{(N-2j-1)(z-2j-1)}. \tag{8.62}$$

Again note that for $z \ll N$, the sum of products is small and as such the first term gives the main contribution. Below is an alternate formulation of the conjecture for even $N, g+\gamma, h+\eta$,

$$\sum_{k=1}^{kmax} 4^k \frac{\binom{\frac{N-g-\gamma}{2}}{k}\binom{\frac{N-h-\eta}{2}}{k}}{\binom{N}{2k}\binom{2k}{k}} = \frac{N-z}{z+1} + \frac{N+1}{z+1} \sum_{k=1}^{\min(g+\gamma,h+\eta)/2} \frac{4^k \binom{(g+\gamma)/2}{k}\binom{(h+\eta)/2}{k}\binom{z/2}{k}}{\binom{N/2}{k}\binom{z}{2k}\binom{2k}{k}} \tag{8.63}$$

since we have

$$\frac{N-z}{z+1} = \sum_{k=1}^{\frac{N-z}{2}} \frac{4^k \binom{(N-z)/2}{k}\binom{N/2}{k}}{\binom{N}{2k}\binom{2k}{k}}. \tag{8.64}$$

Note that the number of terms in the summation is determined by the size of $g+\gamma$ or $h+\eta$. Suppose that $g+\gamma = 0$, then this tells us that the expected number of asymmetric

periodic points is just

$$\frac{N-h-\eta}{h+\eta+1} \qquad \text{or} \qquad \frac{N+1-h-\eta}{h+\eta+1} \tag{8.65}$$

for N even or odd respectively. This is similar to the expected number of periodic points in an s-permutation from chapter 4. We now present a theorem which bounds the number of asymmetric periodic points.

Theorem 8.1.17. *For all N, g, h, γ, η we have*

$$\frac{N-z}{z+1} < \langle \#asymperpt \rangle < \frac{(N-g)(N-h)}{N(z-1)-gh} = \frac{N-z+\psi}{z-1-\psi} \tag{8.66}$$

where $\psi = \frac{(g+\gamma)(h+\eta)}{N}$.

Corollary 8.1.18. *The proportion of points in asymmetric periodic cycles is*

$$\frac{1}{z+1} - \frac{z}{N(z+1)} < \langle P^{asymper} \rangle < \frac{1}{z-1-\psi} - \frac{z-\psi}{N(z-1-\psi)} \tag{8.67}$$

and asymptotically we have

$$\langle P^{asymper} \rangle \to \frac{1}{z}. \tag{8.68}$$

If there are no singularities ($\gamma = 0 = \eta$) this is identical to the result in [64]. In most cases, this proportion will go to 0 but there are (many) non-trivial constructions where this is not the case. The map in equation (8.94) below is an example of a 2D map with $g = 1 = h, \gamma = 0 = \eta$. In this case, we expect half of the space to be consumed in asymmetric periodic points, and the other half to be consumed in symmetric periodic points. In fact, this map has only one symmetric periodic orbit.

We present a lemma which was a basis of the distributional results in [64]. We use it to prove the distribution result for asymmetric cycles and also provide an asymptotic result for the number of asymmetric cycles of length k.

Lemma 8.1.19. *[64] Let k be a fixed integer with $0 < k \leq N/2$. Now fix m with $0 < 2m < N$, and define*

$$\lambda_- = \left(1 - \frac{g+\gamma}{N-m}\right)\left(1 - \frac{h+\eta}{N-m}\right) \qquad \lambda_+ = \left(1 - \frac{g+\gamma-1}{N}\right)\left(1 - \frac{h+\eta}{N}\right) \tag{8.69}$$

and

$$\lambda = \left(1 - \frac{g+\gamma}{N}\right)\left(1 - \frac{h+\eta}{N}\right). \tag{8.70}$$

Then for all k such that $1 \leq k \leq m$ we have

$$\lambda_-^k \leq \prod_{j=0}^{k-1}\left(1 - \frac{g+\gamma-1}{N-(2j+1)}\right)\left(1 - \frac{h+\eta}{N-2j}\right) \leq \lambda_+^k. \tag{8.71}$$

Let $m = m(N)$ be a positive integer sequence such that

$$\lim_{N\to\infty} m(N) = \infty \qquad m = o(N). \tag{8.72}$$

We have $\lambda\pm \approx \lambda$ and hence asymptotically

$$\prod_{j=0}^{k-1}\left(1 - \frac{g+\gamma-1}{N-(2j+1)}\right)\left(1 - \frac{h+\eta}{N-2j}\right) \to \lambda^k. \tag{8.73}$$

We now look at the distribution of the asymmetric periodic orbits given in theorem 8.1.4 which can be can be proved similarly using the combinatorial model.

Proof. Denote $\langle P_k^{asymper}\rangle$ to be the proportion of space in asymmetric periodic orbits of length k. Then from theorem 8.29, using lemma 8.1.19 and dividing by N to get the proportion and summing from 1 to m,

$$\sum_{k=1}^{m}\lambda_-^k \leq \sum_{k=1}^{m}\langle P_k^{asymper}\rangle \leq \sum_{k=1}^{m}\lambda_+^k. \tag{8.74}$$

Putting $m = \lfloor x \rfloor$ we have the distribution function as $N \to \infty$

$$\mathcal{R}_N^{asymper}(x) \approx \sum_{k=1}^{\lfloor x\rfloor}\lambda^k \tag{8.75}$$

$$\approx \frac{1-\lambda^{\lfloor x\rfloor}}{z} \tag{8.76}$$

$$\approx \frac{1-e^{-\lfloor x\rfloor\frac{N}{z}}}{z} \tag{8.77}$$

as required. □

We now consider the asymptotic values for the number of asymmetric cycles of length k.

Theorem 8.1.20. *The number of asymmetric cycles of length k is asymptotically*

$$\langle asymper_k \rangle \to \frac{\lambda^k}{k} \tag{8.78}$$

where λ is given in (8.70).

This follows directly from theorem 8.29 and lemma 8.1.19.

8.1.3 Number of symmetric cycles

We are mainly concerned with the asymmetric cycles since we will see they are the only type of orbit that is useful for detecting integrals so we do not give much attention to the other types of orbits but their statistics may be calculated similarly. We provide a sketch for the number of symmetric periodic orbits below.

Proof. ((8.16) in theorem 8.1.2) A symmetric periodic orbit is characterised by having two points in $\mathrm{Fix}(G) \cup \mathrm{Fix}(H)$. If it contains two points from the one fix set, then it has even length, otherwise if it contains one point from each fix set, then it is of odd length. We count each of these cases. For the odd case with one point each from $\mathrm{Fix}(G)$ and $\mathrm{Fix}(H)$, we have the expected number of symmetric periodic orbits of length $2k-1$ to be

$$\langle \#symper_{2k-1} \rangle = N^{\underline{2k-1}} \frac{\#\mathbf{E}(g-1, h-1, \gamma, \eta, N-2k+1)}{\#\mathbf{E}(g, h, \gamma, \eta, N)} \tag{8.79}$$

$$= \frac{gh}{N-2k+2} \prod_{j=0}^{k-2} \left(1 - \frac{g+\gamma}{N-2j}\right)\left(1 - \frac{h+\eta-1}{N-2j-1}\right) \tag{8.80}$$

$$\approx \frac{gh}{N} \lambda^{k-1} \tag{8.81}$$

and for even length $2k$ with two fixed points in $\mathrm{Fix}(G)$ we have

$$\langle \#symper_{2k} \rangle_g = \frac{N^{\underline{2k}}}{2} \frac{\#\mathbf{E}(g-2, h, \gamma, \eta, N-2k)}{\#\mathbf{E}(g, h, \gamma, \eta, N)} \tag{8.82}$$

$$\approx \frac{g^2}{2N} \lambda^{k-1} \tag{8.83}$$

where we divide by 2 since we count twice all orbits beginning and ending on $\mathrm{Fix}(G)$. This calculation is identical for $\mathrm{Fix}(H)$ where we write h for g,

$$\langle \#symper_{2k} \rangle_h = \frac{N^{\underline{2k}}}{2} \frac{\#\mathbf{E}(g, h-2, \gamma, \eta, N-2k)}{\#\mathbf{E}(g, h, \gamma, \eta, N)} \tag{8.84}$$

$$\approx \frac{h^2}{2N} \lambda^{k-1}. \tag{8.85}$$

Now for each of these, to obtain the total number, we sum over k and taking the asymptotic limit $\sum_{k=1}^{\infty} \lambda^{k-1}$ and then adding the terms together. This yields the value

$$\langle \#symper \rangle = \frac{(g+h)^2}{2N(1-\lambda)} \approx \frac{1}{2} \frac{(g+h)^2}{z}. \tag{8.86}$$

□

A similar procedure can be repeated to obtain the values for the symmetric and asymmetric aperiodic orbits.

Remark 8.1.21. It is important to remember that the calculations above are for the expected value of the composition of two involutions. Although, we expect most reversible birational maps to behave similarly to this, there will be exceptions and various details of the map may invariably give more restrictions on the map than what we expect to see using this probabilistic model. However, we will show that in many cases, this model is a very good guide for the orbit statistics of a reversible map.

Although the results above are for the asymptotic values, we may be interested in how well this approximates the exact value for fixed N. For fixed parameter values, these exact values are complicated expressions involving sums and products but we can compare these to the asymptotic values. The exact value for asymmetric periodic orbits of length k is given by (8.37) compared with the asymptotic value $\frac{\lambda^k}{k}$. Note that the product is approximated better by λ^k for smaller k. We expect the number of asymmetric periodic orbits to converge much faster than the asymmetric periodic points because we are weighting the smaller k. Table 8.1 compares the exact values for the asymmetric periodic orbits and points to the asymptotic values in theorem 8.1.7 and shows its convergence.

Remark 8.1.22. These results give us the expected number as $N \to \infty$. The results here for the asymmetric periodic orbits look similar to the total number of cycles for a

N	Relative error for #asymper	Relative error for #asymperpt
100	1.8979e-03	2.1428e-02
400	3.2702e-04	1.1754e-02
900	1.219e-04	8.0210e-03
1600	6.1357e-05	6.0794e-03
2500	3.6256e-05	4.8927e-03
3600	2.3675e-05	4.0930e-03
4900	1.6551e-05	3.5178e-03
6400	1.2158e-05	3.0842e-03
8100	9.2730e-06	2.7457e-03
10000	7.2839e-06	2.4741e-03

Table 8.1: Comparing asymptotic values for asymmetric periodic orbits and points with the exact expected number for varying N and $g = h = \gamma = \eta = \sqrt{N}$.

Table 8.2: Comparing asymptotic values for symmetric periodic orbits and points with the exact expected number for varying N and $g = h = \gamma = \eta = \sqrt{N}$.

N	Relative error for #symper	Relative error for #symperpt
100	2.0407e-02	2.5640e-02
400	1.0101e-02	1.2658e-02
900	6.7114e-03	8.4033e-03
1600	5.0251e-03	6.2893e-03
2500	4.0161e-03	5.0251e-03
3600	3.3445e-03	4.1841e-03
4900	2.8653e-03	3.5842e-03
6400	2.5063e-03	3.1348e-03
8100	2.2272e-03	2.7855e-03
10000	2.0040e-03	2.5063e-03

random permutation for a fixed space of N points. In fact, from theorems 8.1.2 and 8.1.6, we can write

$$\langle \#asymper \rangle = \log(\langle \#asymperpt \rangle). \tag{8.87}$$

This says that the (expected) number of asymmetric periodic orbits is the log of the (expected) phase space consumed by asymmetric periodic points. This is reminiscent of the result for a random permutation. We also see the Harmonic numbers again in conjecture 8.1.8. Comparing the number of asymmetric cycles of length k, $\approx \lambda^k/k$ for a reversible map, and the number of k-cycles for a random permutation $1/k$, we get

$$\left| \frac{1}{k} - \frac{\lambda^k}{k} \right| = \frac{1}{k}(1 - \lambda^k) = \frac{g + \gamma + h + \eta}{N} + O\left(\left[\frac{g + h + \gamma + \eta}{N} \right]^2 \right). \tag{8.88}$$

using binomial expansion for λ^k. Also if $\frac{g(N)}{N}, \frac{h(N)}{N}, \frac{\gamma(N)}{N}, \frac{\eta(N)}{N} \to 0$ as $N \to \infty$, then we have $\frac{g+\gamma+h+\eta}{N} \to 0$. In general, we will have $N = \mathbb{F}_p^d$ and we will have $\frac{g+h+\gamma+\eta}{N} = O(\frac{1}{p}) \to$

0 as $p \to \infty$. This shows that the cycle structure of the asymmetric orbits of a reversible map is similar to the cycles of a random permutation, and the smaller the cardinality of the fixed sets and singular sets the closer it is. There does seem to be some similarity between asymmetric periodic orbits and cycles in non-reversible maps.

8.1.4 Multiple reversing symmetries or additional symmetries

These results model reversible birational maps L with a single pair of reversing symmetries. It is possible that a map can be written as a composition of different pairs of involutions. For example, suppose L can be written as two distinct pairs of involutions,

$$L = H \circ G, \qquad L = \hat{H} \circ \hat{G} \tag{8.89}$$

where $H, G, \hat{H}, \hat{G}$ are involutions and $H \neq \hat{H}, G \neq \hat{G}$. In this case, we can classify each orbit as being symmetric or asymmetric with respect to each of the pairs of reversing symmetries. Thus, we can categorise cycles into four types. This model does not account for this, however, if one pair of the reversing symmetries has an asymptotic greater growth than the other, using those parameters for the combinatorial model will yield reasonable results. This is because the other symmetry will be in some sense dominated and its effect will not be greatly manifested.

We also note that this may be used to detect reversibility. We will see an example below where some parameters show strong evidence of an additional reversing symmetry by looking at the cycle statistics. In this case, it is visible because we choose a reversible map where the fixed sets of the involutions contain only one point each. Thus, if there is another pair of reversing symmetries with larger cardinalities they will be clearly seen. Maps may also have a symmetry S such that

$$S \circ L = L \circ S. \tag{8.90}$$

In this case, we expect to see more repeated cycles compared to the model.

8.2 Numerical tests for asymmetric orbits in reversible maps

We will compare the results in theorem 8.1.7 for various reversible maps in 2,3 and 4 dimensions. We do not go into much detail for all of the maps as they are simply intended

to show the efficacy of the combinatorial model although we point out some features of the Hénon map and the map 8.2.2. We focus on the asymmetric periodic orbits (and points) since they are not constrained directly by the parameters of the map (in terms of any bounds) and they will be useful for detecting integrals in maps in the next chapter. For the following maps, we provide plots to compare the asymptotic expected number of asymmetric cycles with the observed number.

We follow the notation of Roberts and Lamb in [40] in labelling involutions according to the dimension of its fixed set in $\mathbb{R}^d$. We then label reversible maps according to the labelling of the pair of involutions involved. For example, a type 0-I mapping is a reversible map made up of a type 0 involution and a type I involution, and a type II-II mapping is a reversible map made up of two type II involutions. This will be convenient as the type of involutions control the number of symmetric orbits in a mapping.

For a fixed prime p, we use the result in theorem 8.1.20 and compare the number of asymmetric cycles of length k (for small k) with the observed values. Here, we average over parameter values since the expected number is less than 1 for all k. We also use theorem 8.1.2 and plot the asymptotic expected number compared with the observed value for varying primes p. It is worth noting that the combinatorial approach doesn't depend on dimension, and so we can apply it to any d-dimensional reversible map. We first look at two maps in 2D which we consider in some detail.

Example 8.2.1. We can compare this result of the expected number of asymmetric periodic orbits and points to the reversible Hénon map in 2D over $\mathbb{F}_p^2$ given by

$$L : x' = y, \qquad y' = -x + y^2 + \epsilon \tag{8.91}$$

with parameter ϵ which can be written as $L = H \circ G$ where

$$H : x' = x,\ y' = -y + x^2 + \epsilon, \qquad G : x' = y,\ y' = x \tag{8.92}$$

and H, G are involutions. This is a type I-I map with $g = \#\mathrm{Fix}(G) = p = \#\mathrm{Fix}(H) = h$. There are no singularities so $\gamma + \eta = 0$. In table 8.3 we give the expected and observed values for the number of k-orbits for $p = 1009$ averaged over parameters $\epsilon = 1, \ldots, 1008$. This shows the effectiveness of the model. There is no rigorous reason why we should expect a reversible map to have such similar statistics. Here we average over parameter

values to compare to the model since each of the expected values is less than 1 (and for a map the number of cycles must be discrete). Note that these values of relative error are very good. It would not be unreasonable to see a relative error greater than 1, if there was a value of k where we saw say twice or three times the expected number. One thing we notice though, is the absence of asymmetric cycles of length 1,2,3,4,5. This is one of the shortcomings of this model, as obviously, it cannot account for these properties specific to the map. For a prime p, we also count the number of asymmetric periodic orbits. Figure 8.1 shows the number of asymmetric cycles for $\epsilon = 1$ for primes up to 5000 compared with the asymptotic expected value of $\log(p/2)$. It does seem to be fairly close but due to the discreteness of the cycle count, it's hard to see how good this model is. Thus for each p, we average over parameter values $\epsilon = 1, \ldots, p-1$ and compare with the model. (We exclude $\epsilon = 0$ since it appears that there is another reversing symmetry here.) This is shown in figure 8.3. For the Hénon map, we have an average absolute error of 2.2675 for the number of asymmetric cycles for $p < 5000$. Recall that the number of symmetric cycles is p, and so the relative error for this is small in terms of the total number of cycles. This error is due to the observed property above that there are no cycles of length 1,2,3,4,5. When we take this into account, we get a better fit for the expected number (see the dashed curve in figure 8.3). However, even without this, the number of asymmetric cycles is modelled well we consider the number of symmetric cycles is $p \gg \log(p/2)$. In figure 8.4 we plot the number of asymmetric points compared to the asymptotic expected number of $p/2$ from the model. This is a very good fit. Note that the asymmetric cycles of $1, 2, 3, 4, 5$ contribute little to the number of asymmetric points so this is more robust to "missing" small cycles.

Example 8.2.2. We consider a 2D reversible map $L = H \circ G$ that when reduced to the finite space $\mathbb{F}_p^2$, the involutions H, G have just one fixed point each. We show some results on the number of cycles. We construct this map by letting G be the area-preserving involution given by the negative identity map,

$$G: \; x' = -x, \qquad y' = -y, \tag{8.93}$$

and letting $H = PGP^{-1}$ where we choose P to be a non-linear invertible polynomial map. With this construction, $\mathrm{Fix}(G), \mathrm{Fix}(H)$ have one point each and hence there is one symmetric cycle and the rest of the cycles will be asymmetric periodic orbits. Let us

k	Expected #k-orbits	Observed #k-orbits	Relative Error
1	9.9802e-01	0	1
2	4.9802e-01	0	1
3	3.3136e-01	0	1
4	2.4802e-01	0	1
5	1.9803e-01	0	1
6	1.6470e-01	1.5278e-01	7.2361e-02
7	1.4089e-01	1.6667e-01	1.8298e-01
8	1.2303e-01	1.1905e-01	3.2389e-02
9	1.0915e-01	1.0317e-01	5.4706e-02
10	9.8036e-02	9.3254e-02	4.8782e-02
11	8.8947e-02	8.5317e-02	4.0810e-02
12	8.1374e-02	7.9365e-02	2.4683e-02
13	7.4965e-02	6.3492e-02	1.5305e-01
14	6.9473e-02	5.5556e-02	2.0033e-01
15	6.4713e-02	5.7540e-02	1.1084e-01
16	6.0548e-02	5.7540e-02	4.9685e-02
17	5.6873e-02	3.7698e-02	3.3715e-01
18	5.3607e-02	5.1587e-02	3.7683e-02
19	5.0685e-02	3.7698e-02	2.5623e-01
20	4.8056e-02	5.5556e-02	1.5607e-01

Table 8.3: Comparing asymptotic values for asymmetric periodic orbits of length k given in theorem 8.1.20, that is, $(1-2/p)^k/k$, with the observed number for the Hénon map with $p = 1009$ averaged over parameters $\epsilon = 1, \ldots, p-1$.

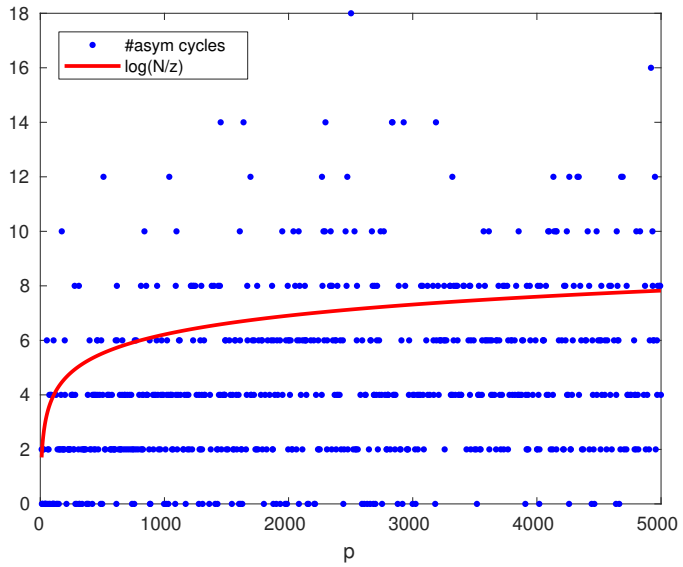


Figure 8.1: Hénon (8.91): Plot of number of asymmetric cycles for $\epsilon = 1$ compared with theorem 8.1.2.

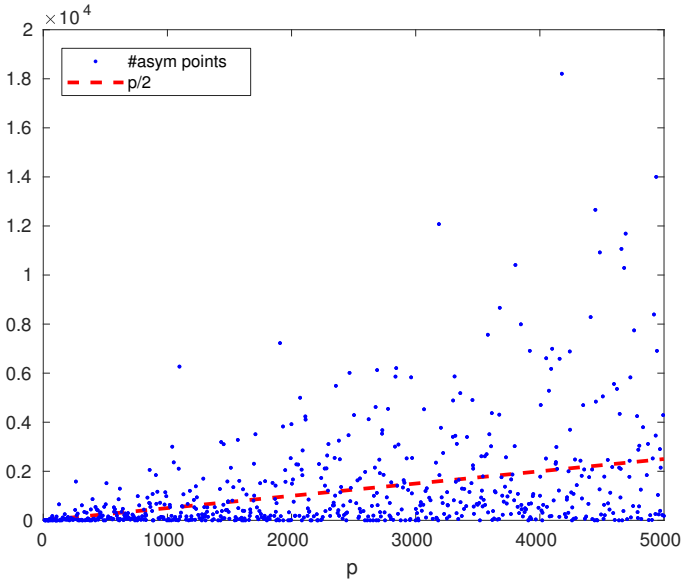


Figure 8.2: Hénon (8.91): Plot of number of asymmetric points for $\epsilon = 1$ compared with corollary 8.1.6.

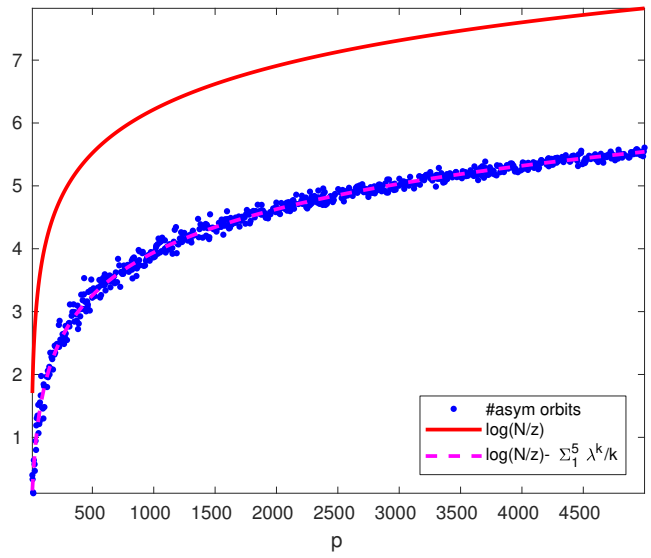


Figure 8.3: Hénon (8.91): Plot of the number of asymmetric periodic orbits averaged over parameters $\epsilon = 1, \ldots, p-1$ for primes from 11 to 4999 (blue) compared to the expected number of $\log(p/2)$ from theorem 8.1.2.

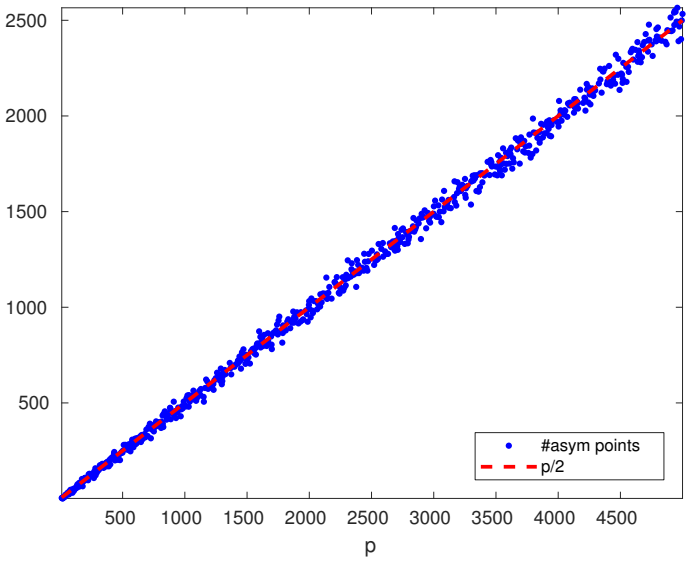


Figure 8.4: Hénon (8.91): Plot of the number of asymmetric periodic points averaged over parameters $\epsilon = 1, \ldots, p-1$ for primes from 11 to 4999 compared to the expected number of $p/2$ from corollary 8.1.6.

choose

$$P: \; x' = x + y^2 + \epsilon, \qquad y' = (x')^2 + y + 2. \tag{8.94}$$

Again, we are interested in the number of cycles of this map. We note that for this map, there seem to be some parameter values which have multiple reversing symmetries. We will discuss this below. Let us first fix $p = 997$. Figure 8.5 shows the number of cycles for each parameter value in the x-axis. There are three spikes in this plot corresponding to three parameter values where there are many more cycles than we expect. For parameters $\epsilon = 2, 387, 608$, we have $999, 1007, 1009$ cycles respectively. This hints that these parameters have an additional pair of reversing symmetries and associated with them are p symmetric cycles. If we subtract $p = 997$ from each of these counts, we get $2, 10, 12$ respectively which is the around the number of asymmetric cycles we would expect for a reversible map on $\mathbb{F}_p^2$ with p symmetric orbits. Thus, even for a reversible map, the cycle count can be indicative of parameters with additional reversing symmetries. We now exclude these three parameter values as they are exceptional. In figure 8.6 we show a histogram of the number of asymmetric cycles. The expected number from the model is $\log(p^2/2) = 13.12$. We see that the distribution is approximately normal, and in particular most values are near this value, and (excluding the three anomalies) the largest parameter value has 30 asymmetric cycles. We can also consider the number of asymmetric cycles of length k. We expect $\frac{\lambda^k}{k}$ asymmetric cycles of length k where $\lambda = (1 - 1/p^2)^2$. This

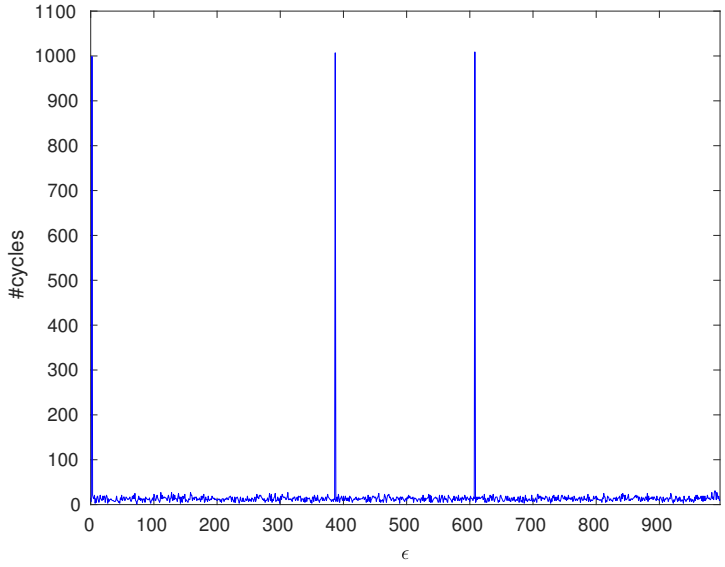


Figure 8.5: Example 8.2.2: Number of cycles for $p = 997$ for parameters $\epsilon = 0, \ldots, p-1$. Note the spikes at $\epsilon = 2, 387, 608$.

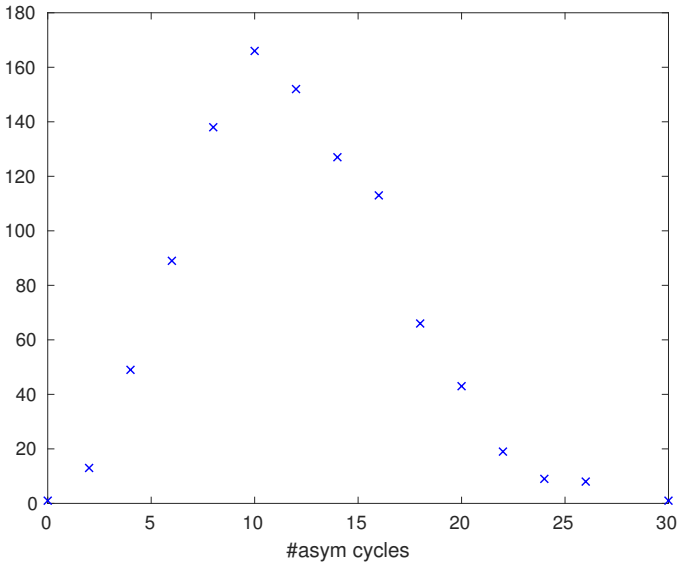
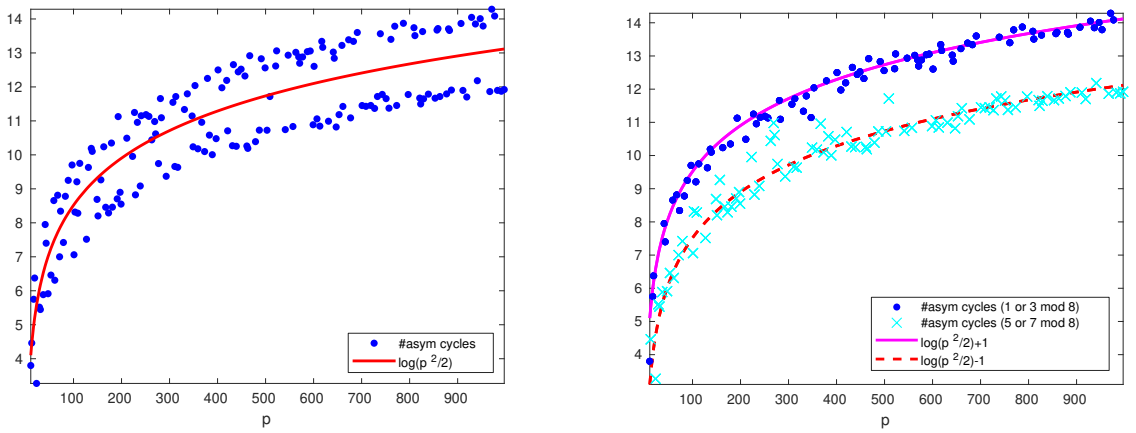


Figure 8.6: Example 8.2.2: Histogram of the number of asymmetric cycles for $p = 997$ considered over all parameters. The vertical axes measure the frequency of occurrence.

is shown in table 8.4 where we have averaged over (non-exceptional) parameter values. From the plot this seems to be fairly accurate except that there are no asymmetric cycles of length 1 for $p = 997$ while we expect around 1. By looking at the cycle lengths of primes, we see that for $p = 1$ or 3 (mod 8) there are two 1-cycles but for $p = 5$ or 7 (mod 8) there are no 1-cycles. However, the model expects about one 1-cycle. Taking this into account, we see that we obtain a better fit for the number of cycles.

k	Expected #k-orbits	Observed #k-orbits	Relative Error
1	1.0000e+00	0	1.0000e+00
2	5.0000e-01	4.9497e-01	1.0056e-02
3	3.3333e-01	3.8229e-01	1.4689e-01
4	2.5000e-01	2.6761e-01	7.0431e-02
5	2.0000e-01	1.7706e-01	1.1468e-01
6	1.6666e-01	1.8511e-01	1.1068e-01
7	1.4286e-01	1.4688e-01	2.8183e-02
8	1.2500e-01	1.2877e-01	3.0198e-02
9	1.1111e-01	9.6579e-02	1.3077e-01
10	9.9998e-02	8.0483e-02	1.9515e-01
11	9.0907e-02	1.0262e-01	1.2880e-01
12	8.3331e-02	8.2495e-02	1.0036e-02
13	7.6921e-02	7.2435e-02	5.8325e-02
14	7.1427e-02	6.6398e-02	7.0396e-02
15	6.6665e-02	8.4507e-02	2.6764e-01
16	6.2498e-02	6.2374e-02	1.9799e-03
17	5.8822e-02	6.4386e-02	9.4605e-02
18	5.5554e-02	5.2314e-02	5.8316e-02
19	5.2630e-02	3.4205e-02	3.5008e-01
20	4.9998e-02	4.4266e-02	1.1465e-01

Table 8.4: Example 8.2.2: Comparing asymptotic values for asymmetric periodic orbits of length k in theorem 8.1.20, that is, $(1-1/p^2)^k/k$, with the observed number for $p = 997$ averaged over parameters $\epsilon = 0, \ldots, p-1$ excluding $\epsilon = 2,387,608$.



(a) (b)

Figure 8.7: Example 8.2.2: The number of asymmetric cycles compared to the expected number of $\log(p^2/2)$ for the combinatorial model in theorem 8.1.2 (left) and the number of asymmetric cycles with $p = 1$ or 3 (mod 8) and $p = 5$ or 7 (mod 8) separated and compared with the model with adjustments (right).

8.2.1 Reversible maps in higher dimensions with no integral

We now consider various maps in 3D with no integral and examine the number of asymmetric periodic orbits. For each particular prime, the number will be few, but we can consider the averaged number over the parameter values and compare it to the model. For the following maps, we only consider the statistic of the number of asymmetric cycles. We could perform similar analysis to the two examples above, and provide various tables and figures for the different statistics and show the histogram over parameter values but it is not of the utmost importance. The analysis performed above was to show that there are certain properties of maps that will not be accounted for in the model but in most cases have a minor effect and can be ignored for the convenience of a simple global and general model.

Example 8.2.3. Consider the 3D map of type I-I called J I-I in example 6.17 in [32] given by

$$x' = -y, \qquad y' = z, \qquad z' = -x + z^2 + y^2 + \epsilon \tag{8.95}$$

which has involutions

$$H:\ x' = y,\ y' = x,\ z' = -z + x^2 + y^2 + \epsilon, \qquad G:\ x' = z,\ y' = -y,\ z' = x. \tag{8.96}$$

This map is a permutation and has $\frac{p+p}{2}$ symmetric periodic orbits. We compare the number of periodic orbits averaged over parameters with the model shown in figure 8.8.

Example 8.2.4. Consider the 3D map type II-II GM. Pert (example 6.13 in [32]) given by

$$x' = y, \qquad y' = z, \qquad z' = x + \frac{y - z}{1 + y^2 z^2} + \epsilon(y^3 - z^3) \tag{8.97}$$

which has involutions

$$G:\ x' = z,\ y' = y,\ z' = x, \qquad H:\ x' = y,\ y' = x,\ z' = z + \frac{y - x}{1 + x^2 y^2} + \epsilon(y^3 - x^3). \tag{8.98}$$

For $p = 3 \pmod 4$ this map is a permutation but for $p = 1 \pmod 4$ there are singular orbits. We show the number of asymmetric cycles averaged over parameters in figure 8.9. Here $N = p^3, g = p^2 = h$ and $\eta = 0$ for $p = 3 \pmod 4$, $\eta = 2p(p-1)$ for $p == 1 \pmod 4$.

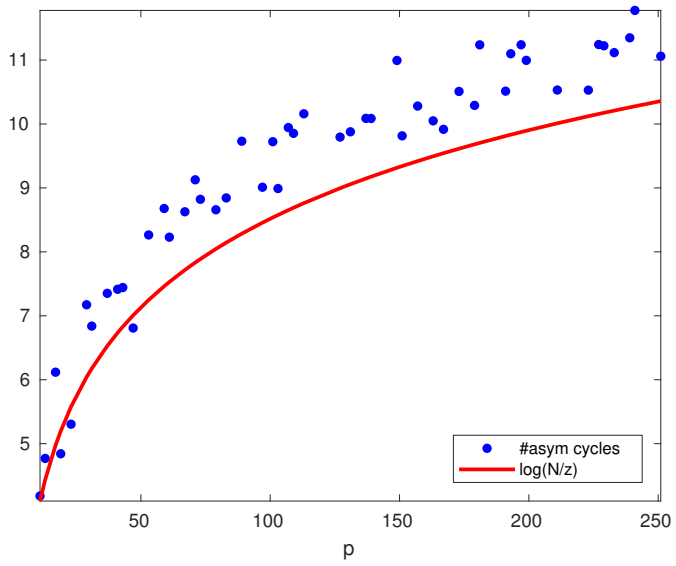


Figure 8.8: Example 8.2.3: The number of asymmetric cycles compared to the expected number of $\log(p^2/2)$ in the combinatorial model from theorem 8.1.2.

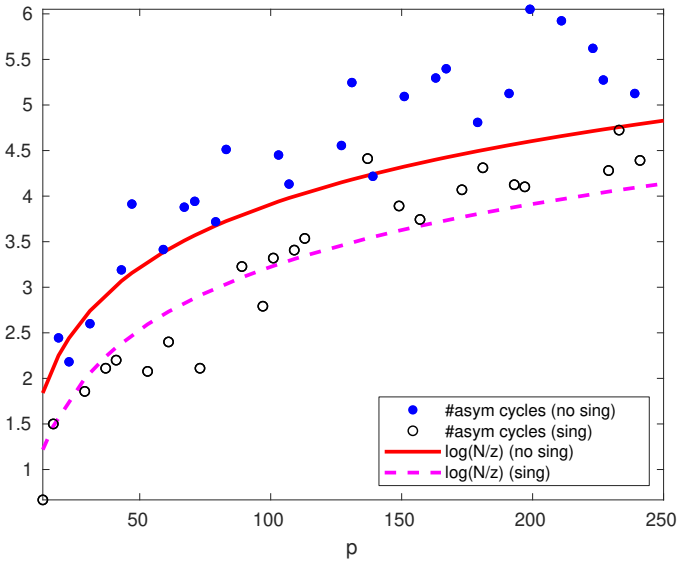


Figure 8.9: Example 8.2.4: The number of asymmetric cycles averaged over $\epsilon = 1, \ldots, p-1$ compared to the expected number of $\log(N/z)$ in the combinatorial model from theorem 8.1.2.

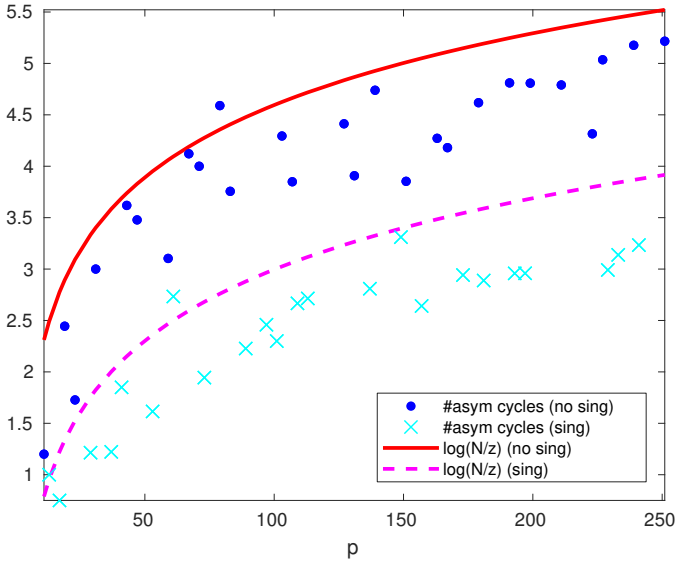


Figure 8.10: Example 8.2.5: The number of asymmetric cycles with $e = 1$ and averaged over $k = 1, \dots p-1$ compared to the expected number of $\log(N/z)$ in the combinatorial model from theorem 8.1.2.

Example 8.2.5. Consider the 3D map type I-II (example 6.14 in [32]) given by

$$\begin{aligned} x' &= (k-y)(1+(y'-1)^2) \\ y' &= \frac{x+e(2y-k)(z+e(y-k))}{1+(y+1-k)^2} \\ z' &= -z+e(k-2y), \end{aligned} \tag{8.99}$$

which has involutions

$$\begin{aligned} &G:\ x' = x+e(2y-k)(z+e(y-k)),\ y' = k-y,\ z' = z+e(2y-k), \\ &H:\ x' = y(1+(y'-1)^2),\ y' = \frac{x}{1+(1-y)^2},\ z' = -z. \end{aligned} \tag{8.100}$$

This map is a permutation for $p = 3 \pmod 4$ and has singular points for $p = 1 \pmod 4$. The number of asymmetric cycles compared with the combinatorial model is shown in figure 8.10 with $e = 1$ and averaged over parameters $k = 1, \dots p-1$. For this map we have $N = p^3, g = p^2, h = p, \gamma = 0$ and $\eta = 0$ for $p = 3 \pmod 4$, $\eta = 4p(p-1)$ for $p = 1 \pmod 4$.

Example 8.2.6. Consider the 4D type II-II map (example 6.20 in [32]) given by

$$w' = w - 3y^2 + 2yz,\ x' = x - 6z^2 + y^2 - \epsilon,\ y' = y + w',\ z' = z + x' \tag{8.101}$$

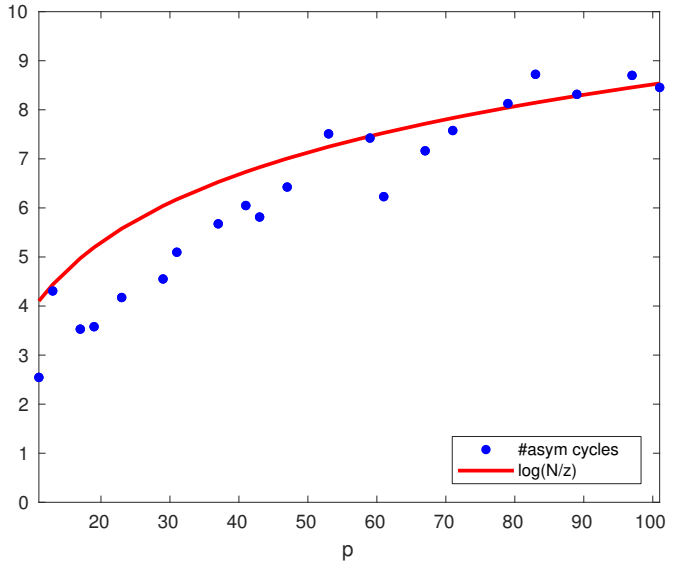


Figure 8.11: Example 8.2.6: The number of asymmetric cycles for varying primes averaged over $\epsilon = 0, \ldots, p-1$ compared to the expected number of $\log(N/z)$ in the combinatorial model from theorem 8.1.2.

which has involutions

$$G: \ w' = -w, \ x' = -x, \ y' = y - w, \ z' = z - x,$$
$$H: \ w' = -w + 3y^2 - 2yz, \ x' = -x - y^2 + 6z^2 + \epsilon, \ y' = y, \ z' = z.$$

This map is a permutation of the space and the number of asymmetric cycles averaged over parameter values is shown in figure 8.11. Here $N = p^4, g = p^2 = h, \gamma = 0 = \eta$.

8.3 Concluding Remarks

In this chapter, we presented a combinatorial model for the statistics of reversible maps. We extended the model of Roberts and Vivaldi in [64] by accounting for singularities and in particular, focusing on the number of asymmetric cycles and points which was not considered previously. Although, in general, the number of asymmetric cycles is very small compared to the symmetric cycles and their proportion vanish, we are able to obtain meaningful results. Numerical tests to check the model are simple to perform as obtaining the number of asymmetric cycles requires an orbit decomposition of the map in a finite space, while calculating the expected number from the model requires the cardinality of the fixed points and singular points. We provided numerical tests to show the model seems to be a good estimator for the number of asymmetric cycles for various types of maps in different dimensions, with and without singularities. It is with this confidence

that we will present a test for integrals based on this in the following chapter. We see that after filtering out symmetric cycles (and singular orbits), the statistics of the asymmetric cycles are indicative of the number of algebraic integrals present in a map.

Chapter 9

Detecting integrals in d-dimensional reversible maps

In this final chapter, we use the number of asymmetric periodic orbits as a discriminator for the number of integrals by providing a heuristic for this number based on the ideas and results in chapter 3, 4, 6 and 8. The basis of this heuristic is that the combinatorial models are good in approximating the statistics for (reversible) maps. We will also be able to model maps with integrals by modifying the parameters in these models and considering multiple copies of a reduced system. This proves to be effective despite simplifying assumptions for which there seems to be no easy way around. (This has been a common technique throughout the literature.) However, many times we see maps behaving like random maps with similar constraints (e.g. see [8, 47, 57]). This culminates in a practical algorithm for detecting the number of integrals in reversible maps of any dimension. We apply this to a menagerie of reversible maps from the literature and show its efficacy.

9.1 Modelling reversible maps with integrals

In the previous chapter, we considered a combinatorial model for various statistics of reversible maps. This model assumed that the map in some sense is constrained only by its reversibility, that is, it has no other (known) algebraic properties like an integral or other (reversing) symmetries. We want to see if we can use this idea to also model the statistics for reversible maps with integrals. Suppose we are given a d-dimensional reversible (algebraic) map $L = H \circ G$ with $j > 0$ integrals that are rational (the case with $j = 0$ was considered in chapter 8). We reduce to the finite space $\mathbb{F}_p^d$ and consider the number of orbits we see. Let N, g, h, γ, η be the value of size of the space, fixed set of G, fixed set of H, singular set of G, singular set of H respectively. How can we account for the

fact that now there are j integrals? There will now be p^j level sets defined by the j-tuple $(l_1, l_2, \ldots, l_j)$ where l_i is the value of the ith level set where each $l_i \in \mathbb{F}_p$. For convenience, we can define the level set value $\Lambda = \sum_{i=1}^{j} l_i p^{i-1}$ where each $l_i \in \{0, \ldots, p-1\}$ and hence $0 \leq \Lambda \leq p^j - 1$, and talk about the level set with value Λ to mean a particular j-tuple. For each level set we will have the four types of orbits described by being either symmetric or asymmetric and either periodic or aperiodic. In terms of the combinatorial model, we can think of a reversible map with j integrals as p^j reversible systems of reduced size for its phase space, fixed sets and singular sets.

Let $N_i, g_i, h_i, \gamma_i, \eta_i$ be the values of the reduced parameters for the the level set with $\Lambda = i$ corresponding to number of points on the level set, fixed set of G, fixed set of H, singular set of G, singular set of H respectively. Clearly, we must have

$$\sum_{i=0}^{p^j-1} Q_i = Q, \tag{9.1}$$

for $Q = N, g, h, \gamma, \eta$. Similarly, we can also let $\#symper_i, \#asymper_i, \#asymaper_i, \#symaper_i$ be the number of each type of orbit on the ith level set where we must have

$$2\#symper_i + \#symaper_i = g_i + h_i \tag{9.2}$$

and

$$\#symaper_i + \#asymaper_i = \gamma_i + \eta_i. \tag{9.3}$$

However, when we consider the total number over all level sets, the #symper, #asymaper, #symaper are not affected by the presence of integrals. For example, if $\gamma + \eta = 0$ then the symmetric cycles are given by the sum of the number of symmetric cycles on each level set, that is,

$$\sum_i \frac{g_i + h_i}{2} = \frac{g + h}{2} \tag{9.4}$$

independent of the number of integrals j. In general, this is also the case as the parameters g, h, γ, η constrain the number of orbits of each type whether there are integrals or not. So, these three types of orbits cannot be used to differentiate the presence of integrals. This leaves us with asymmetric cycles. These are not constrained by these parameters (as we also noted in the case with no integrals). We examine the effect of integrals of this number.

9.2 Asymmetric cycles for reversible maps with integrals

Recall from the previous chapter for a reversible map with no integrals we have in theorem 8.1.2 and 8.1.20 the expected number of asymmetric cycles of length k and asymmetric cycles asymptotically as

$$\langle \#asymper_k \rangle = \frac{\lambda^k}{k} \tag{9.5}$$

$$\langle \#asymper \rangle = \log\left(\frac{N}{z}\right). \tag{9.6}$$

Now suppose that a reversible mapping $\hat{L}$ defined on a space of N points possesses j integrals of motion. Then each point and orbit will lie on a j-tuple $(l_1, \ldots, l_j)$ of the level sets. The points on the fixed sets and singular sets must also be distributed among the level sets. To proceed, we present a lemma which will be the basis of our model for the number of asymmetric cycles and points.

Assumption 9.2.1. Suppose that the number of fixed points and singular points distributed on each level set is proportional to the number of points on the level set. So for each i we have

$$\frac{N_i}{g_i} = \frac{N}{g}, \qquad \frac{N_i}{h_i} = \frac{N}{h}, \qquad \frac{N_i}{\gamma_i} = \frac{N}{\gamma}, \qquad \frac{N_i}{\eta_i} = \frac{N}{\eta} \tag{9.7}$$

and hence

$$\frac{N_i}{z_i} = \frac{N}{z}. \tag{9.8}$$

Then on each level set indexed by i the expected number of asymmetric cycles and points is

$$\langle \#asymper \rangle_i = \log\left(\frac{N_i}{z_i}\right) = \log\left(\frac{N}{z}\right) \tag{9.9}$$

$$\langle \#asymperpt \rangle_i = \frac{N_i}{z_i} = \frac{N}{z} \tag{9.10}$$

which is independent of the level set i.

The big caveat here is if the assumption is ever satisfied or if not, if it is a reasonable one. It is generally not satisfied except in artificially constructed cases. Essentially, it is saying that the ratio of the various special points on the level sets is the same as the global ratio. Even if this is not true, it is not unreasonable that we expect this ratio to be

relatively constant. For example, the Hasse-Weil bound in higher dimensions give some uniformity of the size of the levels sets. If so, this result says that the expected number of asymmetric cycles and points on a level set is independent on the level set i, and is equal to the expected number of asymmetric cycles and points of a map with the same parameters but no integrals where the expected number is $\log(N/z)$ as in theorem (8.1.2). This differs from the other three types of orbits for which we would expect each level set to only have a small proportion when compared the case with no integrals.

Corollary 9.2.2. *It follows directly from theorem 9.2.1 that the expected number of asymmetric cycles and asymmetric periodic points on $\hat{L}$ is given by*

$$\langle \#asymper \rangle = p^j \langle \#asymper \rangle_i = p^j \langle \#asymper \rangle = p^j \log\left(\frac{N}{z}\right) \tag{9.11}$$

$$\langle \#asymperpt \rangle = p^j \langle \#asymperpt \rangle_i = p^j \langle \#asymperpt \rangle = p^j \frac{N}{z}. \tag{9.12}$$

Similarly, we can consider asymmetric periodic orbits and points of length k and by the assumptions in (9.7) we get that $\lambda_i = \lambda$.

Corollary 9.2.3. *The expected number of asymmetric orbits and points of length k is given by*

$$\langle \#asyperorb_k \rangle = p^j \frac{\lambda^k}{k} \tag{9.13}$$

$$\langle \#asyperpt_k \rangle = p^j \lambda^k. \tag{9.14}$$

Note that the above results also apply for reversible maps with no integrals ($j = 0$) as they reduce exactly to the results in chapter 5. Although, reversible maps with an integral will not satisfy the conditions in assumption 9.2.1, corollary 9.2.2 and 9.2.3 are still good heuristic models in general for the asymmetric cycle and point statistics. This is because the conditions are still approximately equal. In fact, using the combinatorial model for

each level set we have

$$\sum_{i=1}^{p^j} \log\left(\frac{N_i}{z_i}\right) < p^j \log\left(\frac{1}{p^j}\sum_{i=1}^{p^j}\frac{N_i}{z_i}\right) \tag{9.15}$$

$$\approx p^j \log\left(\frac{N}{z}\right) \tag{9.16}$$

where the first line is due to the AM-GM inequality. The second line relies upon the N_i and z_i being relatively equidistributed among the level sets. The inequality is not important to us but these equations give some justification for being able to use (9.11). Similar arguments can be used for the other equations.

9.3 Detecting integrals in reversible maps

We now present the main result of this chapter which use the results in corollary 9.2.2 and 9.2.3 to form a test for the number of integrals in a reversible map. Supposing that this accurately models the statistics of asymmetric orbits and points in a reversible map with j integrals, by replacing the expected number in this model by the observed number in a reversible map and making j the subject in the above equations, we obtain estimates for the number of integrals j. That is, using the number of asymmetric cycles, we have from (9.11) and (9.12),

$$j^* = \frac{\log(\#asymper) - \log\log(N/z)}{\log p} \tag{9.17}$$

and using the asymmetric points, we have

$$j^* = \frac{\log(\#asyperpt) - \log(N/z)}{\log p}. \tag{9.18}$$

Using asymmetric cycles is more robust to (anomalous) long asymmetric cycles but may be sensitive to (anomalous) repeated small asymmetric cycles (of a specific number). Conversely, using the asymmetric periodic points is robust to having (anomalous) repeated small asymmetric cycles but sensitive to (anomalous) long asymmetric cycles. These are practical and useful results as finding the number of asymmetric cycles and points is easy for appropriately chosen prime p. This is the advantage of working in the finite field as we can find these numbers by performing an orbit decomposition of the space in finite time. Note that we also have control of prime p chosen. In fact, for different primes, we

will obtain different estimates j^* (but of course it should be near-integer in value). Thus, by considering a reversible map for various primes p, we can check the consistency and accuracy of the obtained values

Additionally, for a fixed prime p, we can obtain a test for the number of asymmetric orbits of length k using corollary 9.2.3 as

$$j_k^* = \frac{\log(k\#asymper) - k\log\lambda}{\log p}. \tag{9.19}$$

This should be more accurate for smaller k as the data will be less sparse. This will also show how accurate the model is on a smaller level. We would expect that using the number of all asymmetric cycles or points would be more accurate as it is in a sense averaging over all k. We will not use this as this is zooming in and gives multiple values for a chosen prime but just mention it in passing.

Our result can be useful because integral detection is an important area of research [27]. This result can be used to estimate the numbers of integrals in a reversible map. It will be most effective for maps that do not have any other constraining properties (which may be hard to know beforehand). It is simple in the sense that no difficult calculations need to be carried out. We note that this test is quite robust in that the number of asymmetric cycles do not need to be that close to the expected number to have good results. This is because the model has a factor of p^j which means that for each extra integral, we expect a factor of p more cycles which is significant. Thus for reasonably sized prime p, if the map gives us two or three times more asymmetric cycles than expected the value of j^* would still be close to the true value. Explicitly, for a d dimensional rational map, we do the following:

1. Pick a prime p.
2. Calculate the parameters g, h, γ, η.
3. Perform a full orbit decomposition of the map in $\mathbb{F}_p^d$, counting the number of asymmetric cycles.
4. Compute j^* from (9.17) [or (9.18)].
5. (Optional) Repeat steps 1-4 for a different prime p.

9.3.1 Similarity to the model in section 6.6

This model for the number of asymmetric cycles assumes that level sets "look similar", and in essence, the presence of integrals gives us a stack of copies of a reversible map with reduced parameters. However, in chapter 6 we saw that the QRT map (a reversible map with an integral) had additional structure. All cycles on level sets had the same cycle length and this value varied for different level sets. We presented a basic model which gave us an estimate of the number of asymmetric cycles in (6.95). By making j the subject we obtained a test for integrals in (6.96). Comparing the two, since

$$\log\left(\frac{N}{z}\right) \leq \log\left(\frac{N}{g/2+h/2+\gamma+\eta}\right) \leq \log\left(\frac{N}{z}\right) + \log 2. \tag{9.20}$$

Then by comparing (9.17) and (6.96), for large p, we have that $\bar{j^*} \to j^*$. This gives us support to combine these two different models into one. We do this because given a reversible map (with integrals), we in general do not know a priori the behaviour of the cycles on level sets. This allows us to perform this calculation without discrimination or need of selecting a particular model. Thus for all reversible maps we use the 5 step procedure described above.

9.4 Numerical tests for reversible maps

We perform the above steps for a variety of reversible maps where the number of integrals is known. We show that the model for the asymmetric cycles is good and hence the test for the number of integrals is good. We also consider the distribution of the symmetric and singular points over the level sets for some maps to show their distribution has a nice "bell shape" which justifies the approximation in (9.16).

9.4.1 Hénon map 2D

The first map we consider is the Hénon map considered in example (8.2.1). This map has no integrals and figures 8.1,8.2 show the number of asymmetric cycles and asymmetric points respectively. We can also use these numbers to obtain a value for the estimate of the number of integrals j^* shown in figure 9.1. The scarcity and discrete nature of the asymmetric cycles (and points) is reflected in the plot. Here we see that the asymmetric cycles give a more consistent estimate. This is generally true as this statistic is not affected by the length of the cycles as the asymmetric points are, which seems to have a higher

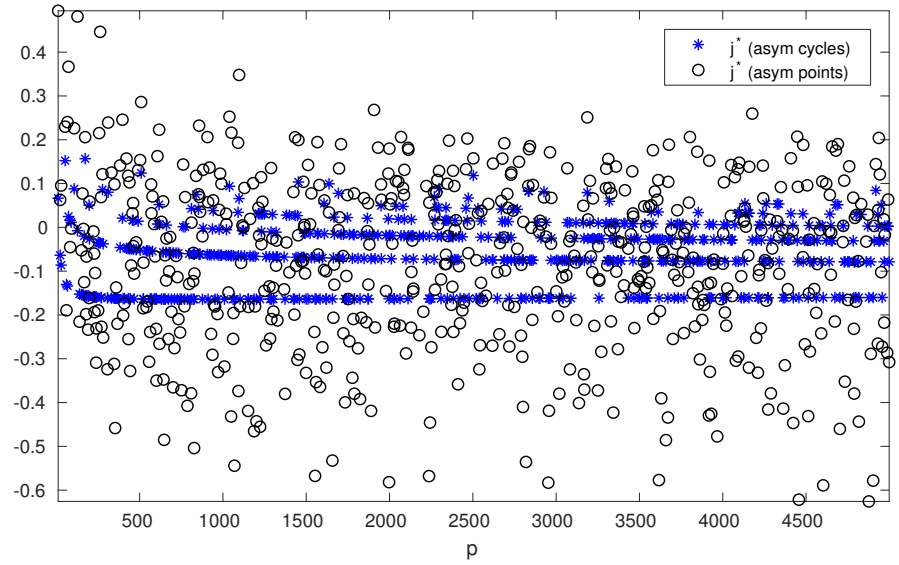


Figure 9.1: Hénon map (8.91): Plot of the j^* in (9.17) and (9.18) for primes from 11 to 4999

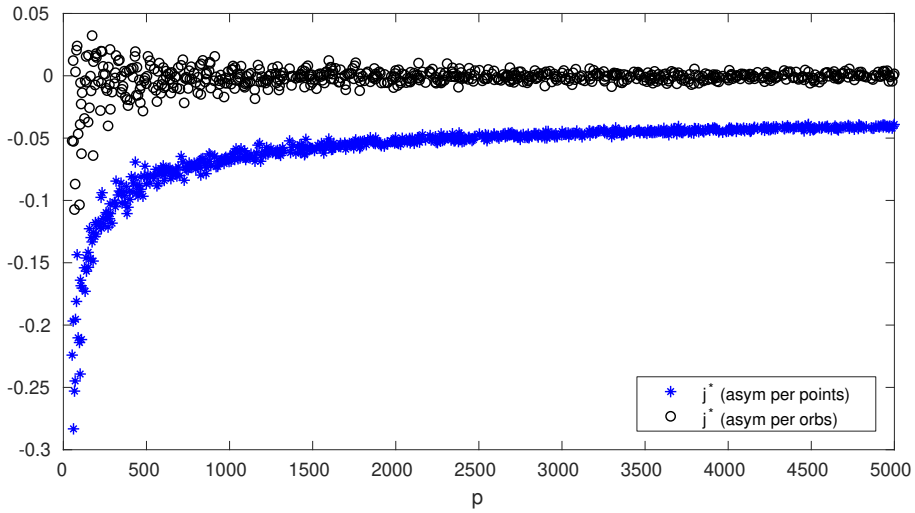


Figure 9.2: Hénon map (8.91): Plot of the j^* in (9.17) and (9.18) where we averaged the number of asymmetric cycles and points over parameter values $\epsilon = 1, \ldots, p-1$ in (8.91) for primes from 53 to 4999.

variance. Additionally, the primes with 0 asymmetric cycles and points are not shown as they are assumed to be non-zero for the formulas and j^* is undefined for them.

It is worth noting that if we average over parameter values, we will obtain smooth plots as the number of asymmetric cycles (and points) will no longer be discrete. (This is similar to what we did in the previous chapter in figure 8.4 and 8.3.) This is shown in figure 9.2 where we see the values indicating 0 integrals.

9.4.2 Hénon map 3D

We first consider here a simple example to illustrate the idea of this model for estimating the number of integrals for a reversible map. We construct a reversible map with 1 integral where the conditions of (9.7) hold, that is, we have $\frac{N_i}{z_i} = \frac{N}{z}$ for every level set i. Thus, we expect the model to be good. This reversible map is derived from the Hénon map in (8.91) but we add a third coordinate to get the following map with an integral,

$$L : x' = y, \qquad y' = -x + y^2 + z, \qquad z' = z. \tag{9.21}$$

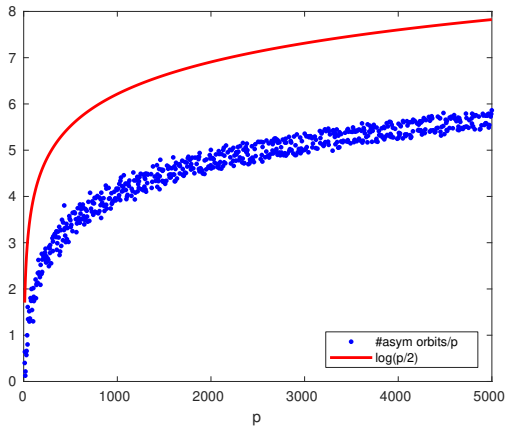
We have replaced the parameter ϵ with z and created a "trivial" integral $I(x, y, z) = z$. Each level set of this map is the 2D Hénon map with parameter determined by the value of z. In this case, we will have p level sets each with p^2 points. This map is just p copies of the 2D Hénon map considered over each of the p parameter values. This has reversing symmetries H, G such that $L = H \circ G$,

$$H : x' = x,\ y' = -y + x^2 + z,\ z' = z, \qquad G : x' = y,\ y' = x,\ z' = z. \tag{9.22}$$

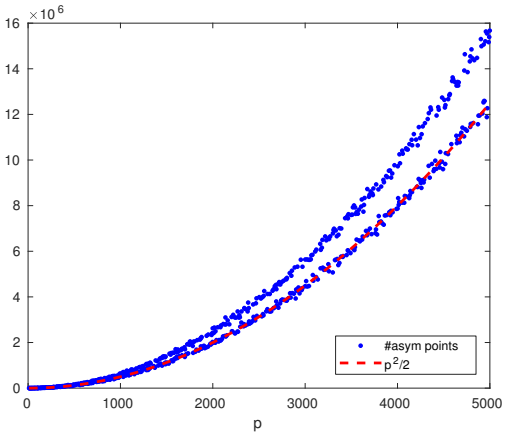
Thus, we have $N = p^3, g = p^2, h = p^2$ and $\gamma = 0 = \eta$ since there are no singularities. Thus, $z = g + h + \gamma + \eta = 2p^2$ and we expect the number of asymmetric cycles to be

$$p \log\left(\frac{N}{z}\right) = p \log\left(\frac{p}{2}\right). \tag{9.23}$$

Similarly, we expect $\frac{p^2}{2}$ asymmetric periodic points. These values are shown in figure 9.3 where for the asymmetric cycles, we have divided by p to see the behaviour better. We can also think of dividing by p as obtaining the average number of asymmetric cycles on level sets. The appearance of two "lines" in the figures is that for the level set $I(x, y, 0) = 0$ some primes p have many more asymmetric cycles than expected. This may be the sign of some additional structure. In figure 9.4 we plot the value of j^* from the tests for integrals in (9.17) and (9.18) showing that the asymmetric statistics point to 1 integral. This example shows the idea in general that of reversible maps with j integrals being p copies of reduced "reversible systems".



(a) Hénon 3D: The number of asymmetric cycles divided by p compared with the value from the model $\log(p/2)$.



(b) Hénon 3D: The number of asymmetric periodic points compared with the value from the model $p^2/2$.

Figure 9.3

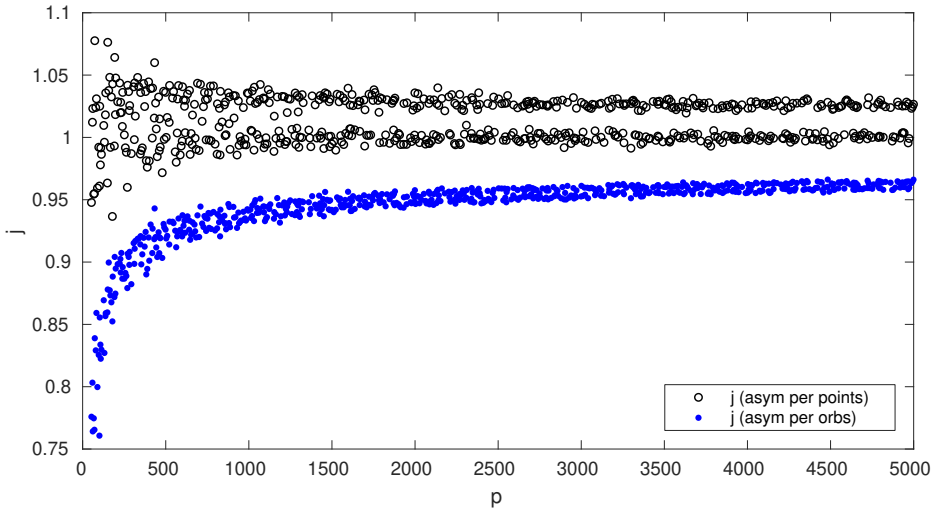


Figure 9.4: Hénon 3D: Plot of j^* in (9.17) and (9.18) for primes from 53 to 4999.

9.4.3 GM 3D

We now consider a 3D map called GM (example 6.9 in [32]) which is type II-II with one integral. It is given by

$$x' = y, \qquad y' = z, \qquad z' = x + \frac{y - z}{1 + y^2 z^2}. \tag{9.24}$$

Note that this map is the map in example 8.2.4 when $\epsilon = 0$. This map has an integral of motion

$$I(x, y, z) = x^2 + y^2 + z^2 + xy + yz - xz + x^2 y^2 z^2. \tag{9.25}$$

and is the composition of involutions H, G with

$$H : x' = y,\ y' = x,\ z' = z + \frac{y - x}{1 + x^2 y^2}, \qquad G : x' = z,\ y' = y,\ z' = x. \tag{9.26}$$

Here we have $N = p^3, g = p^2 = h$. For $p = 3 \pmod 4$ there are no singularities and so $\gamma = 0 = \eta$ but for $p = 1 \pmod 4$ there are singularities and we have $\gamma = 0, \eta = 2p(p-1)$. There are p level sets corresponding to the p values of the integral I. In contrast to the 3D Hénon map previously, the values of the reduced parameter values $N_i, g_i, h_i, \gamma_i, \eta_i$ are not all the same on level sets. We will investigate how the dynamics of this map breaks down into its level sets in terms of these parameters and the numbers of cycles.

We will investigate the distribution of these values for $p = 601$. For this prime there are singularities. We will first examine a particular level set and zoom out gradually to look at the distribution of values on the level sets, and then finally the total number of asymmetric cycles and points of the whole map. Firstly, consider the level set corresponding to $I(x, y, z) = 227$. The number of points on this level set is the number of solutions $(x, y, z) \in \mathbb{F}_p^3$ to the equation $I(x, y, z) = 227$ which is 363204 points. We can also find the number of these points in the fixed sets of G, H and the singular sets of G, H which we denote by $g_{227}, h_{227}, \gamma_{227}, \eta_{227}$ respectively. For $p = 601$ we find that

$$N_{227} = 363204,\ g_{227} = 594,\ h_{227} = 560,\ \eta_{227} = 1196,\ \gamma_{227} = 0. \tag{9.27}$$

We can use these parameter values for the combinatorial model in theorem 8.1.2. This will give us expected values for the number of orbits of each type. This is shown in table 9.1 for the level set $I(x, y, z) = 227$. This is typical of what we see for any level set for

orbit	model	actual
asymmetric cycles	5.04	2
symmetric cycles	282.34	268
symmetric aperiodic	608.69	618
asymmetric aperiodic	587.31	578

Table 9.1: GM3D (9.24): The expected number from the combinatorial model and the actual number for $p = 601$ and the level set $I(x, y, z) = 227$.

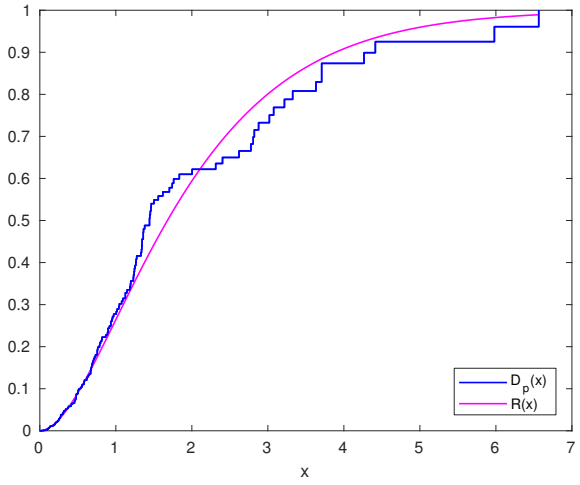
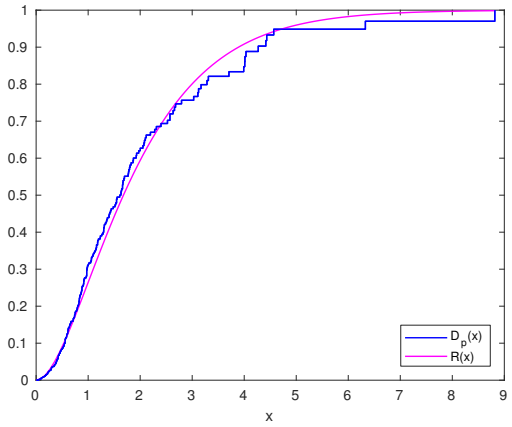


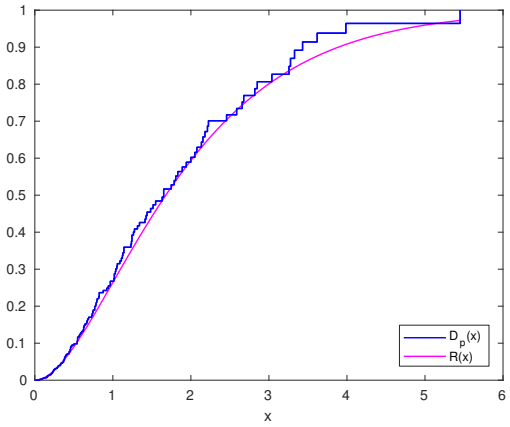
Figure 9.5: GM3D (9.24): Distribution of the lengths of symmetric cycles for $p = 601$ on the level set $I(x, y, z) = 227$. Here there are 268 symmetric cycles with mean length 322.67.

this map. We also consider the distribution of the different types of orbits compared to theorem 8.1.4. This is shown in figure 9.5 for symmetric cycles and figure 9.6 for symmetric and asymmetric singular orbits (left and right respectively).

Now we zoom out one level and look at the distribution of these statistics over level sets. Each level set will have different numbers for the parameters, and for the numbers of each type of orbit. For $p = 601$, we find that the number of points on the 601 level sets lie between 358044 and 367398. The distribution is shown in figure 9.7. Note that $358044/601^2 = 0.9913$ and $367398/601^2 = 1.0172$ so the number of points do not differ much from the average value of 601^2. We provide plots for the prime $p = 601$ to show the break down of the level sets in terms of number of points in $\mathrm{Fix}(G) \cup \mathrm{Fix}(H)$ and $\mathrm{Sing}(G) \cup \mathrm{Sing}(H)$, denoted on each level set by $g_i + h_i$ and $\gamma_i + \eta_i$ respectively in figure 9.8. We also plot a histogram of the ratio N_i/z_i which represents the expected number of asymmetric points on the level set with value i and also the corresponding plot with log applied to the x-axis to represent the expected number of asymmetric periodic orbits on the level set with value i.



(a) GM3D (9.24): Distribution of the lengths of symmetric singular orbits for $p = 601$ on the level set $I(x, y, z) = 227$. Here there are 618 symmetric singular orbits with mean length 299.83.



(b) GM3D (9.24): Distribution of the lengths of asymmetric singular orbits for $p = 601$ on the level set $I(x, y, z) = 227$. Here there are 578 asymmetric singular orbits with mean length 157.56.

Figure 9.6

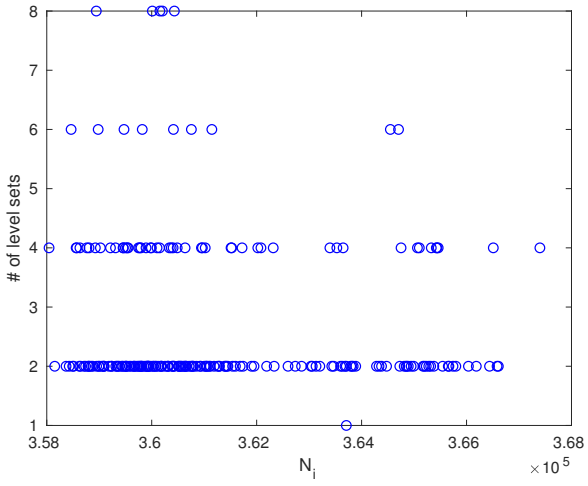
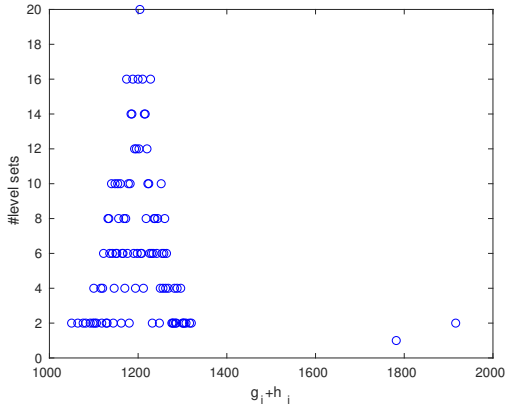
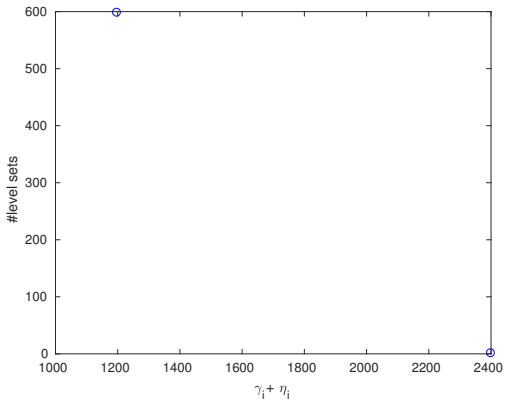


Figure 9.7: GM3D (9.24): The distribution of the number of points on level sets for $p = 601$.

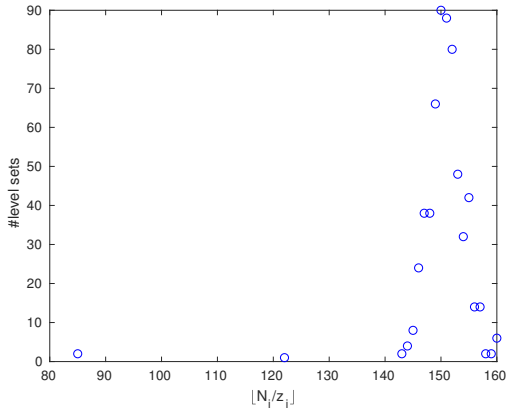


(a) GM3D (9.24): We consider the distribution of the symmetric points over the level sets (that is, those fixed under the involutions G or H). This is for $p = 601$ where there are $2p^2$ symmetric points and p level sets for the full space. All the level sets have between 1065 and 1325 symmetric points except for one with 1646 (corresponding to $I(x, y, z) = 0$).

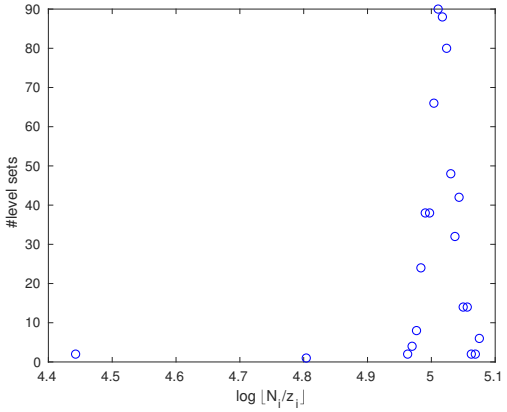


(b) GM3D (9.24): We consider the distribution of the singular points over the level sets. This is for $p = 601$ where there are $2p(p-1)$ singular points and p level sets for the full space.

Figure 9.8

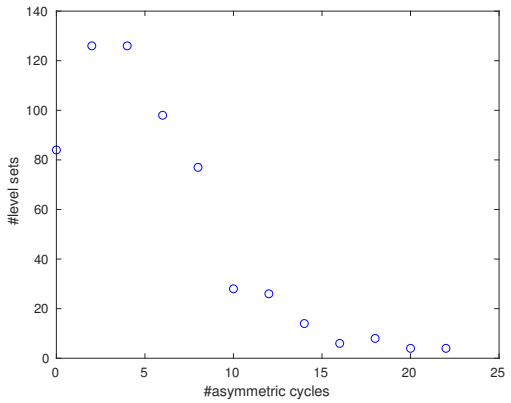


(a) GM3D (9.24): This shows the ratio $\lfloor N_i/z_i \rfloor$ where the parameters are the reduced values on the level sets. We have $p = 601$. Here we have $N/z = 150.71$ for the full space. We took the floor function for purposes of the histogram.

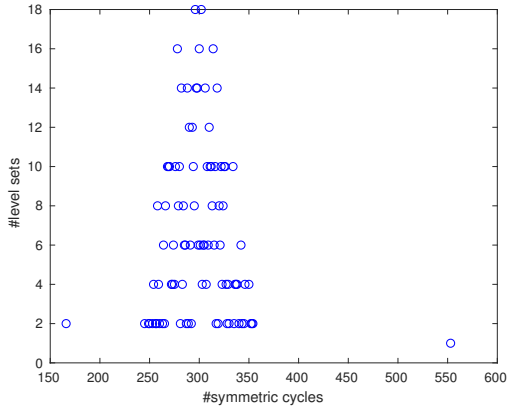


(b) GM3D (9.24): The same plot as left but log is applied to the x-axis to show the histogram of the expected number of asymmetric cycles on level sets using the reduced parameter values.

Figure 9.9



(a) GM3D (9.24): Histogram of the number of asymmetric cycles over the level sets for $p = 601$. Here it ranges from 0 to 22. The mean number of asymmetric cycles on a level set is 5.25. Note that $\log(N/z) = 5.01$. Here we have 3156 asymmetric cycles and $p\log(N/z) = 3013$.



(b) GM3D (9.24): Histogram of number of symmetric periodic orbits per level set for $p = 601$. The expected number averaged over the number of level sets is given by 299.26.

Figure 9.10

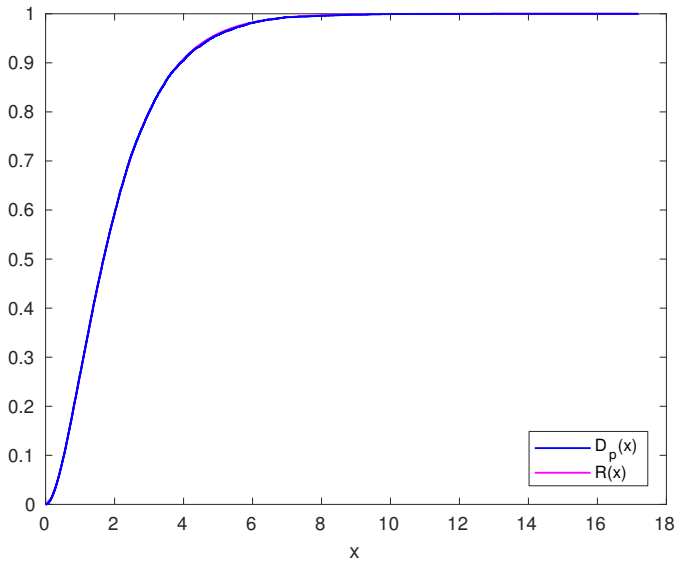
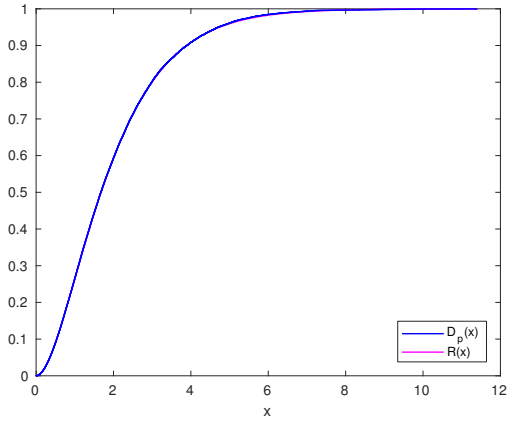
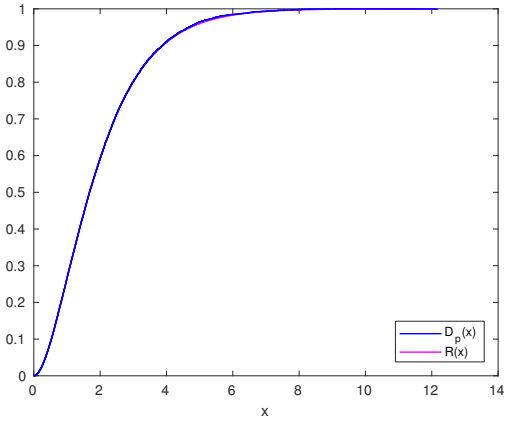


Figure 9.11: GM3D (9.24): Cumulative distribution of symmetric periodic orbit lengths for $p = 601$ scaled by the number of symmetric orbits compared with $\mathcal{R}(x)$. They are virtually indistinguishable.

In figure 9.10 we plot the distribution of the number of asymmetric periodic orbits and symmetric periodic orbits on each level set using a histogram. We also see that the distribution of the three types of orbit lengths follows $\mathcal{R}(x)$ shown in figures 9.11 and 9.12. This shows that the model works well for predicting many of the orbit statistics and supports the idea that we can view this map as p copies of a smaller system.



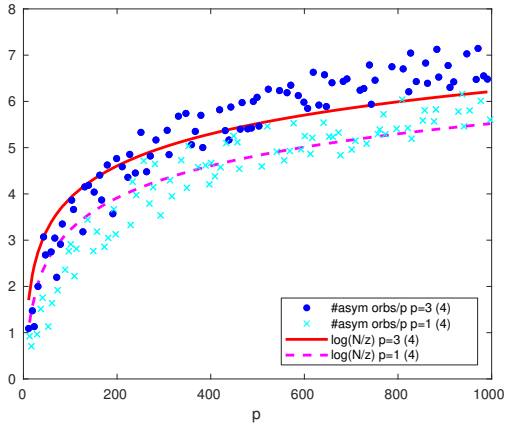
(a) GM3D (9.24): Cumulative distribution of symmetric aperiodic orbit lengths for $p = 601$ scaled by the number of symmetric singular orbits compared with $\mathcal{R}(x)$. They are virtually indistinguishable.



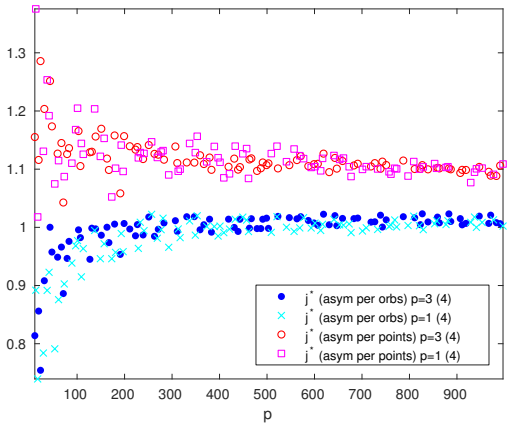
(b) GM3D (9.24): Cumulative distribution of asymmetric aperiodic orbit lengths for $p = 601$ scaled by the number of asymmetric singular orbits with $\mathcal{R}(x)$. They are virtually indistinguishable.

Figure 9.12

These results for the level sets show that the various parameters are fairly evenly distributed, and so the idea of having p copies of reversible systems with phase spaces and fixed sets, and the use of the average values is justified. Finally, for varying primes p, we consider the number of asymmetric cycles averaged over the level sets compared with the expected value of $\log(N/z)$ in figure 9.13a. Here we see the difference in the values for those primes with and without singularities. The integral test using asymmetric cycles and asymmetric points is also shown for primes with no singularities or singularities in figure 9.13b. The values being close to 1 shows that the number of asymmetric cycles are a good indicator of the number of integrals by using our model. We show that both the asymmetric periodic points and cycles give good results. Notice that we did not require any knowledge of the integral to do these calculations. It also shows that this test works well irrespective of whether there are singularities or no singularities.



(a) GM3D (9.24): Plot of the number of asymmetric periodic orbits divided by p for primes 11 to 997.



(b) GM3D (9.24): Plot of j^* in equations (9.17) and (9.18) for primes from 11 to 997.

Figure 9.13

9.4.4 eq51 (j=1 or 2)

This is a 4D map (equation 5.1 in [12]) given by

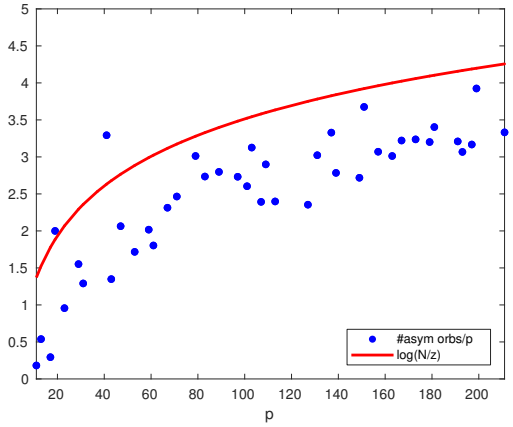
$$\begin{aligned} L:\ w' &= x, \\ x' &= y, \\ y' &= z, \\ z' &= \frac{1}{w}\frac{[xz(y+a_5)a_2h_2+(y+a_6)h_6]}{[xyz(y+a_1)h_1+y(y+a_2)h_2]} \end{aligned} \tag{9.28}$$

which has involutions

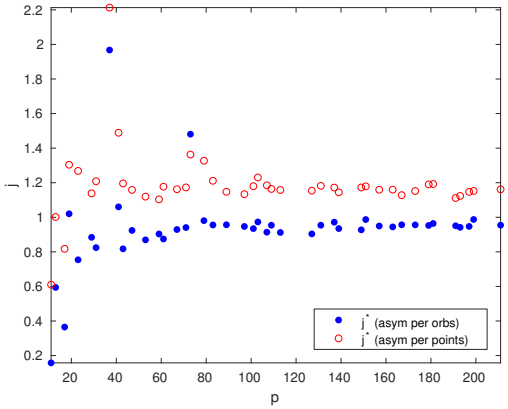
$$\begin{aligned} G:\ w' &= z, & H:\ w' &= y \\ x' &= y, & x' &= x \\ y' &= x, & y' &= w \\ z' &= w & z' &= \frac{1}{z}\frac{[wy(x+a_5)a_2h_2+(x+a_6)h_6]}{[wxy(x+a_1)h_1+x(x+a_2)h_2]} \end{aligned} \tag{9.29}$$

where H is defined for $wxy(x+a_1)h_1+x(x+a_2)h_2 \neq 0$ and $wy(x+a_5)a_2h_2+(x+a_6)h_6 \neq 0$. For general a_1, a_2, a_5 and a_6 with $a_2a_5 = a_1a_6$ this mapping has one integral. However, for the following two possibilities

$$h_2 = 0, \qquad h_1 \neq 0, \qquad h_6 \neq 0, \tag{9.30}$$



(a) eq51j1 9.28: Plot of the average number of asymmetric periodic orbits on each level set for eq51 with $j = 1$.



(b) eq51j1 9.28: Plot of the j^* in (9.17) and (9.18) for eq51 with $j = 1$.

Figure 9.14

and

$$h_1 = h_6 = 0, \qquad h_2 \neq 0 \tag{9.31}$$

the mapping has two independent integrals. Over the finite space $\mathbb{F}_p^4$ the values of the parameter values for $\mathrm{Sing}(G), \mathrm{Sing}(H), \mathrm{Fix}(G), \mathrm{Fix}(H)$ differ depending on the parameter values but in general, $N = p^4, g = p^2, h = O(p^2), \gamma = 0, \eta = O(p^3)$. For numerical tests in figure 9.14, we chose $a_1 = 4, a_2 = 6, a_5 = 2, a_6 = 3, h_1 = \alpha, h_2 = 5, h_6 = 2$ so there is only one integral. In figure 9.14a the values for $p = 37, 73$ are outside the limits of the plot with values 84.05 and 24.96 respectively. For $p = 37$ there are 3110 asymmetric cycles where 3076 are of length 12. For $p = 73$, there are 1822 asymmetric cycles where 1656 are of length 3. This explains the unusual values for these two primes. This model cannot account for specific lengths where there are an exceptional number of cycles as this is not the expected behaviour. This suggests that the map for those specific combination of primes and parameters has a property that allows it to have many copies of a cycle length. However, in figure 9.14b for most primes, we see that the model suggests that there is 1 integral.

We also do similar figures for the map with two integrals. We chose parameters $a_1 = 7, a_2 = 3, a_5 = 4, a_6 = 2, h_1 = 1, h_2 = 0, h_6 = 2$. The numerical tests are shown in figure 9.15. For this case we see many more asymmetric cycles. We will also provide numerical support that the other types of orbits cannot be used to differentiate the number of integrals. Table 9.2 compares the numbers of the different types of orbits for various primes

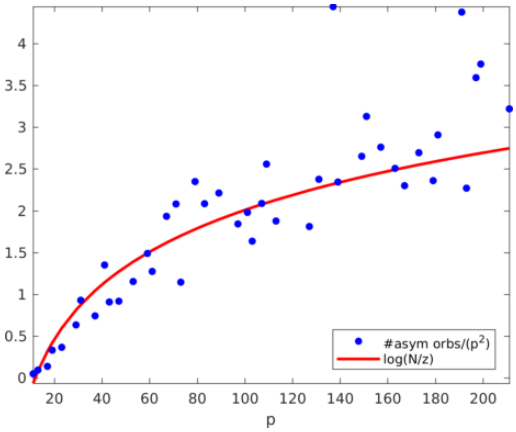
prime	#asym cyc (j=1)	#asym cyc (j=2)	#sym cyc (j=1)	#sym cyc (j=2)
31	40	894	24	57
61	110	4746	47	145
101	263	20222	73	287
131	396	40830	94	380
163	491	66684	129	352
181	616	95346	152	518
211	703	143462	155	545
prime	#asym sing (j=1)	#asym sing (j=2)	#sym sing (j=1)	#sym sing (j=2)
31	109940	164934	1874	1687
61	864606	1307210	7137	7031
101	4000850	6029974	20055	20427
131	8788780	13231380	34193	35641
163	17059378	25592492	52847	48545
181	23329534	35087716	64891	67005
211	37133933	55701070	87941	86271

Table 9.2: eq51 9.28: Comparison of the number of asymmetric cycles,symmetric cycles, asymmetric singular orbits and symmetric singular orbits for the map eq51 for parameters corresponding to $j = 1$ and $j = 2$ integrals.

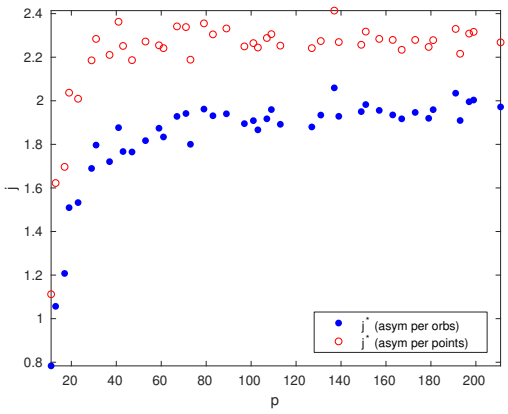
for parameters corresponding to $j = 1$ or $j = 2$ integrals. The symmetric cycles, symmetric singular orbits and asymmetric singular orbits differ only by a constant ratio which cannot help us to detect the number of integrals. This is actually just due to differences in the parameters g, h, γ, η for the different choices of a_i, h_i for the map. However, for the asymmetric cycles we see significant differences in number which differ by a ratio of about p (for $j = 1$ to $j = 2$) - see figure 9.14b versus figure 9.15b. This illustrates clearly the idea of the model we presented at the beginning of this chapter that additional integrals increase the number of asymmetric cycles by a factor of p. Thus, for example, suppose we did not know the conditions for two integrals given in (9.30) and (9.31), by looking at the number of asymmetric cycles it is possible to find out these conditions because they would give us many more asymmetric cycles than expected (for the same map with one integral).

9.4.5 QRT Map

We refer again to the QRT map in (6.58). It is easy to show that $g = p = h$ for $p \equiv 3 \pmod 4$ and $g = p - 2 = h$ for $p = 1 \pmod 4$. Also for $p = 3 \pmod 4$ there are no singularities but for $p = 1 \pmod 4$ we have $\gamma = 2p = \eta$. As mentioned in subsection 9.3.1, although we had the model given in (6.95), we can simply use (9.17) and (9.18) to estimate the number of integrals, and corollary 9.2.3 for the number of asymmetric



(a) eq51j2 9.28: Plot of the average number of asymmetric periodic orbits on each level set for eq51 for $j = 2$.



(b) eq51j2 9.28: Plot of j^* in (9.17) and (9.18) for eq51 with $j = 2$.

Figure 9.15

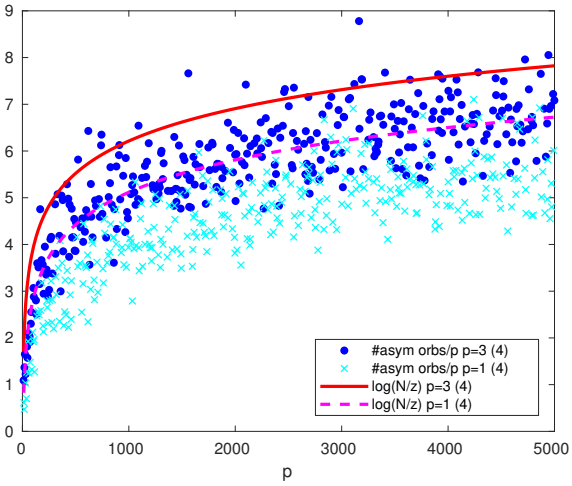
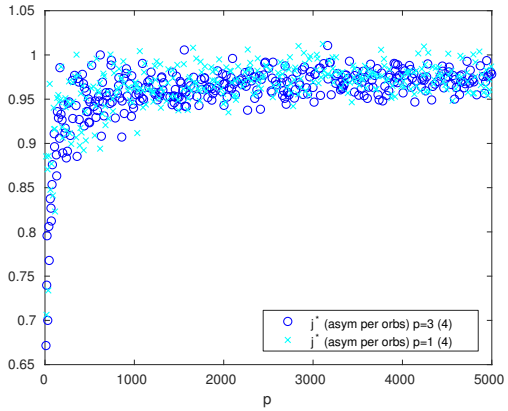
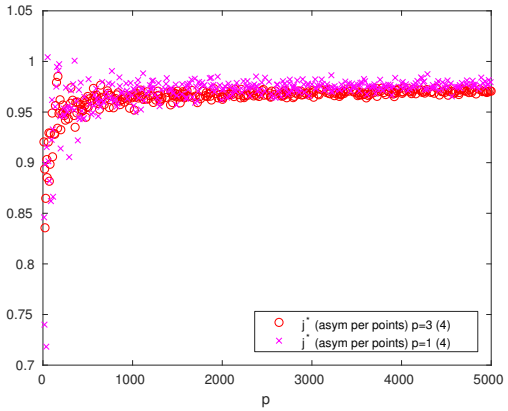


Figure 9.16: QRT (6.58): The number of asymmetric periodic orbits divided by p compared to the model in corollary 9.2.2.

points and cycles. Figure 9.16 shows the number of asymmetric cycles for the QRT map compared with the expected numbers using corollary 9.2.2. We separate the primes into those with and without singular points and provide the two different lines for each corresponding case. In figure 9.17 we provide the estimate for the number of integrals j^* using asymmetric cycles (left) and asymmetric periodic points (right) for primes from 11 to 4999. This clearly shows that we see approximately the number of asymmetric cycles and points we expect for a map with the parameters N, g, h, γ, η of the QRT map.



(a) QRT (6.58): The number of asymmetric cycles divided by p to estimate the number of integrals j as in (9.17).



(b) QRT (6.58): Using the number of asymmetric periodic points to estimate the number of integrals j as in (9.18).

Figure 9.17

9.4.6 L3 Map

The map L3 [60] is a 4D map with $j = 2$ integrals and type II-II reversibility. It is given by

$$\begin{aligned} L3: \quad w' &= y \\ x' &= z \\ y' &= x + K[1/(1+y) - 1/(1+z)] \\ z' &= -w - x + K[1/(1+z) - 1/(1-y-z)] \end{aligned} \tag{9.32}$$

with reversing symmetry given by

$$\begin{aligned} G: \quad w' &= z & H: \quad w' &= x \\ x' &= y & x' &= w \\ y' &= x & y' &= y + K[1/(1+x) - 1/(1+w)] \\ z' &= w & z' &= -z - y + K[1/(1+w) - 1/(1-x-w)]. \end{aligned} \tag{9.33}$$

Here we have $N = p^4, g = p^2, h = p^2, \gamma = 0, \eta = 3p^2(p-1)$. Figure 9.18 shows the average number of asymmetric cycles for each level set, and figure 9.19 shows the values of j^*.

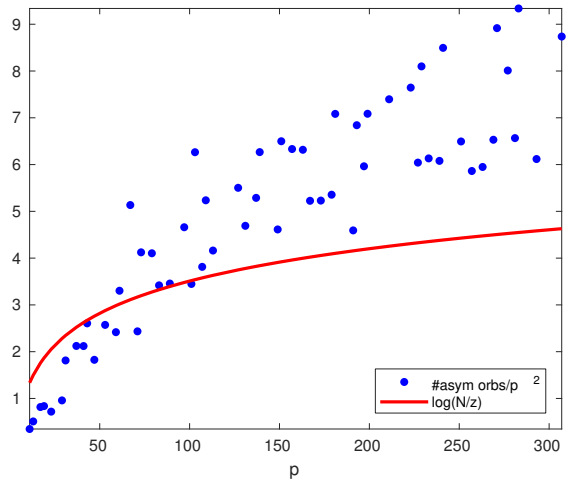


Figure 9.18: L3 (9.32): The number of asymmetric periodic orbits divided by p^2 compared to the model.

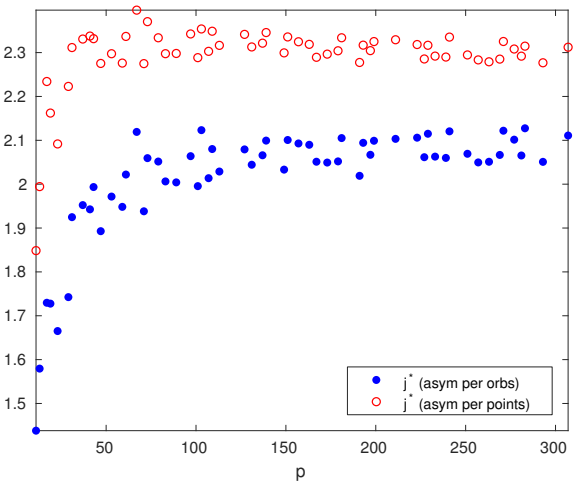


Figure 9.19: L3 (9.32): Plot of j^* in (9.17) and (9.18) for primes from 11 to 293.

9.4.7 CS311 Map

The map CS311 (equation 3.11 in [12]) is a 4D map with $j = 3$ integrals and type II-II reversibility. It is given by

$$\begin{aligned} w' &= x \\ x' &= y \\ y' &= z \\ z' &= w\frac{(\kappa_1 y + \lambda_1)xz + (\kappa x + \lambda_1 z)(y+1) + (\lambda_1 y + \kappa_1)}{(\kappa_1 y + \lambda_1)xz + (\kappa_1 z + \lambda_1 x)(y+1) + (\lambda_1 y + \kappa_1)}. \end{aligned} \tag{9.34}$$

Here we have $g = p^2, h = p^2, \gamma = 0, \eta = p^2(p+1)+1$. We look at the square of the map CS311. This is because we noticed that half of the level sets had no points and noticed

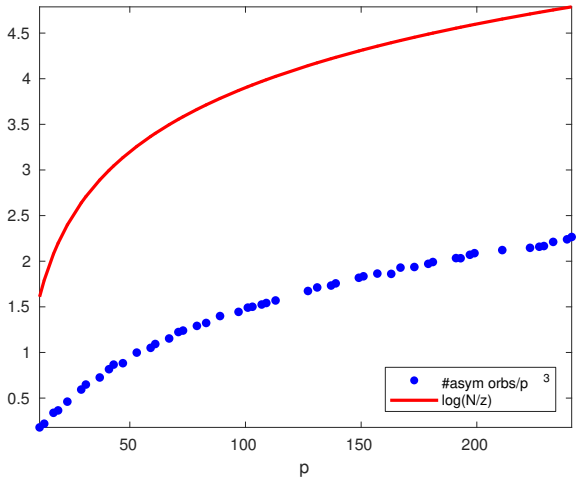


Figure 9.20: CS311 (9.34): The number of asymmetric periodic orbits divided by p compared to the model.

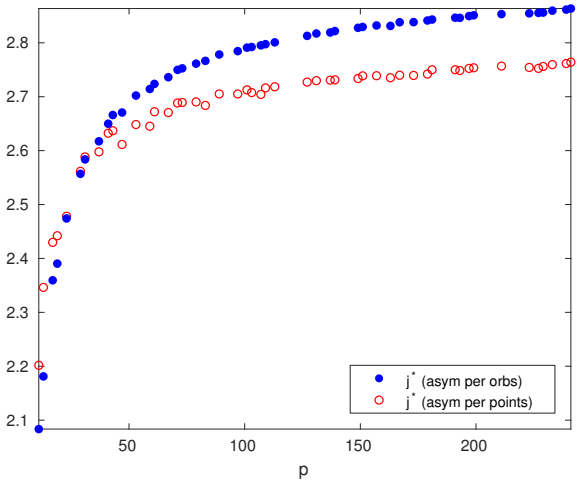


Figure 9.21: CS311 (9.34): Plot of j^* from (9.17) and (9.18) for primes from 11 to 241.

that there were many more even periodic orbits compared to odd periodic orbits. Looking at the square of CS311 gives us very similar numbers of asymmetric periodic orbits as what we expect for each k.

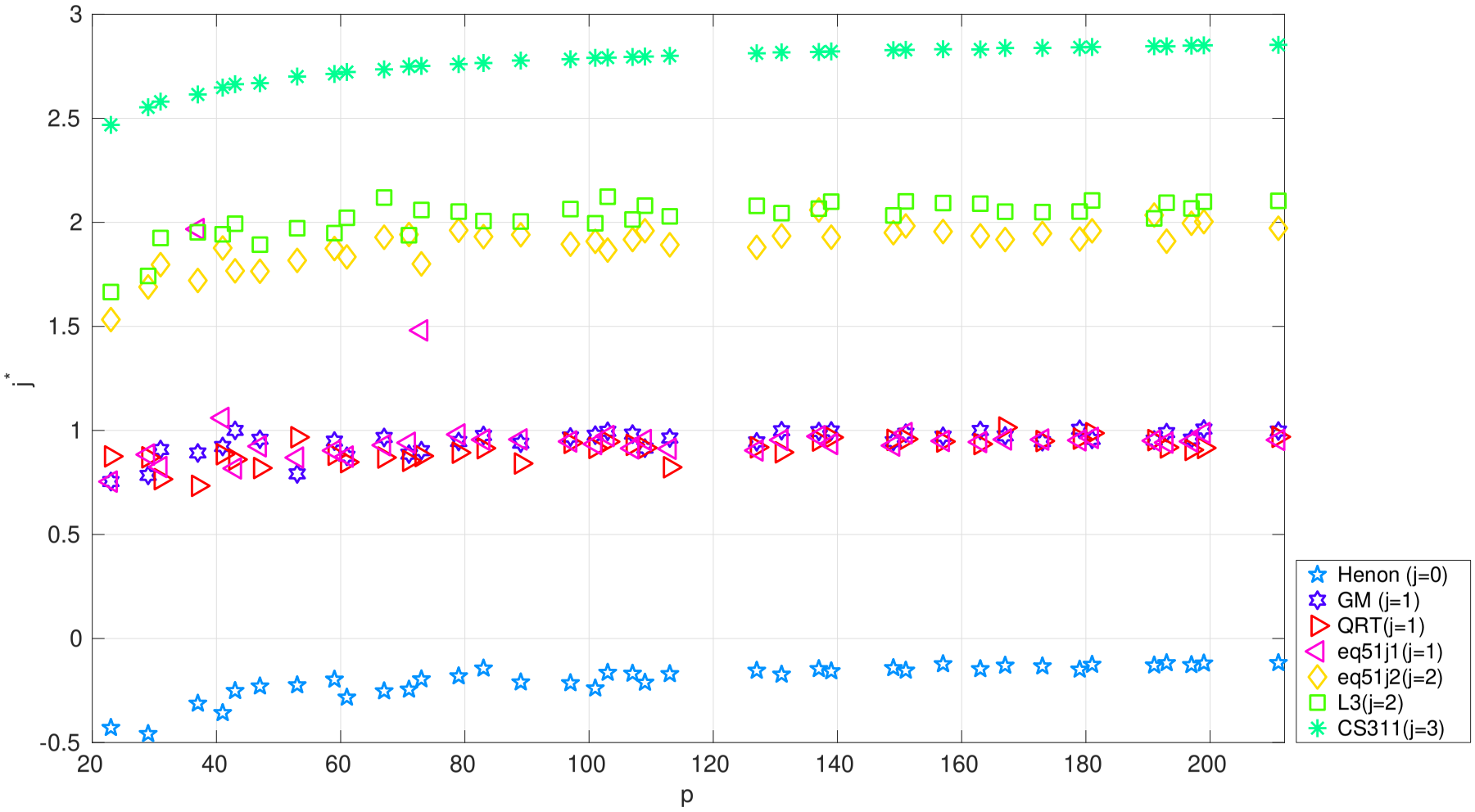


Figure 9.22: Combining the plot of j^* for a range of reversible maps for primes from 19 to 211 showing the efficacy of this model. The known number of integrals j is shown in the legend.

9.5 Concluding remarks

In this chapter, we provided a test for the number of integrals j for birational reversible maps. From the numerical tests, we see that this test gives agreeable answers to the true answer. Note that this test is done without any prior knowledge of the integrals of the map. We considered some reversible birational maps (with integrals) in detail to show the basis of the model. In many cases, the breakdown of map into the level sets defined by the integral gives us p^j copies of a reversible map on a reduced space. Thus, by using the expected numbers of orbit statistics for reversible maps obtained in chapter 8 we could also estimate (relevant) orbit statistics for reversible maps with integrals. This was predicated on the idea that the various parameters would be relatively equidistributed on the level sets. In general, this is what happens, and we showed for the example of the GM map, the distributions of the various statistics which justifies the idea of the model. We turned the expected statistics for asymmetric cycles and asymmetric periodic points into an estimate for the number of integrals j^* in (9.17), (9.18) and showed that due to the similarity to the model in chapter 6, we could use all the estimates and expected values from this chapter for any reversible birational map. Figure 9.22 is the culmination of this chapter comparing the result of the test for various birational reversible maps. This figure shows the test works extremely well in estimating the number of integrals. For each map, there is a clear trend of the values of j^* toward the integer value corresponding to its number of integrals. We also see that this test is independent of the prime p chosen. This indicates the orbit statistics are on the whole largely dependent on the number of points in the space, fixed points and singular points, rather than the specific details of the map or the prime for which the map is being reduced on. In practice, one could pick a handful of primes for which to calculate j^* and if they all give a value close to the same integer, that would give a strong indication of the number of integrals.

This method is not foolproof though, as for example, if the map has many other symmetries or some structure giving it many cycles of a specific length, this test may not work well. This was observed for the map eq51 (9.28) with $j = 1$ for $p = 37, 73$ (and specific parameters) we obtained many more asymmetric cycles than expected. This could be a sign of other symmetries or constraining behaviour. In these exceptional cases it will be difficult to have a general test using orbit statistics will be able to determine the number of integrals accurately. There may be ways by digging deeper into the specific asymmetric

cycle lengths to filter out specific unusual behaviour or to give these less weighting in the overall value of j^*. Our test is based on the observation that reversible maps are constrained mainly by the reversing symmetries and integrals and not the particular details of the map, and that maps with the same constraints have similar statistics. Thus, we also expect the statistics to be close to the expected value of these classes of maps. This model requires that the main structures in the map are its reversibility and integrals.

Chapter 10

Conclusion

In this thesis, we studied the orbit statistics of dynamical systems over finite fields. We were particularly interested in reversible maps and the property of possessing integrals. This started modestly with an introduction followed by some definitions and examples with each chapter building on concepts and ideas of the previous ones. Thus, chapters 7, 8, 9 is the culmination of my research and is all original work (although chapter 4 is also entirely original and 6 also has some original work).

This adventure began in chapter 2 with general maps over finite fields, and then considering the special cases of polynomial automorphisms or birational maps. In chapter 3 we reviewed some results on random permutations and compared them with polynomial automorphisms showing a strong connection in their number of cycles. This idea of using or comparing combinatorial models with polynomial (or rational) maps has been utilised to great effect in the past, for example in Pollard's factorisation algorithm [57]. We take full advantage of this building further combinatorial models for our maps in the future chapters. This was done immediately in chapter 4 where we extended the random permutation model for *random s-permutations*. We obtain some nice summation results in counting the number of cycles and cyclic points. Finally, we compared this model with some birational maps showing their close agreement. All the results in this chapter were original. This laid the foundation for the following chapters. Polynomial automorphisms or birational maps can possess the property of being *reversible*. Reversibility and some basic consequences were presented in chapter 5. Integrals of motion were introduced in chapter 6 with some examples. We provided in-depth analysis on the effects of integrals on the orbit statistics for a few different maps that indicated what may occur in general.

In chapter 7 we studied a family of piecewise linear maps which can be seen as a simple reversible perturbation of linear reversible maps. (Any linear map which is unimodular is reversible and the dynamics can be solved completely and the orbit statistics is known as seen in chapter 6.) By observing this map, we can see the departure from a linear map, and in particular, the distribution of normalised periods appears to change from a singular distribution (for a linear map) to the gamma distribution $\mathcal{R}(x) = 1 - e^{-x}(1 + x)$. This distribution has appeared in [63] where it was conjectured to be the limiting distribution for reversible planar polynomial automorphisms over $\mathbb{F}_p^2$ and in [64] where it was shown to be the expected distribution for the composition of two involutions (satisfying some mild conditions). It was also conjectured in [52] to be the asymptotic distribution of the Casati-Prosen map.

In chapter 8, we revisited the combinatorial model in [64]. Here, we generalised it to include singular points (analogous to the extension of the model in chapter 4 from random permutations to random s-permutations). This was important because most higher dimensional reversible maps have singular points. We shifted our focus to the number of asymmetric orbits and points which were not previously considered in detail. We compared the results from this model with various reversible maps and show that they seem to be effective in predicting the number of asymmetric cycles in reversible maps.

Finally, in chapter 9, we provided a test for the number of integrals in a reversible birational map. This was based on the results and ideas in the previous chapters, and required only the calculation of the number of asymmetric cycles in the orbit decomposition. We justified the simplifying assumptions required for this model by considering a range of reversible maps in high dimensions over the finite field. We also showed the efficacy of this test by comparing its prediction for the number of integrals for these maps with the known values. The advantage of this test is that it is simple to perform and yields good results for many maps. The difficulty is that it cannot account for properties (other than reversibility and integrals) that may alter the orbit statistics of the map such as other symmetries. Anomalies in the test, however, suggest further investigations are needed.

References

[1] S. Ahmad. Cycle structure of automorphisms of finite cyclic groups. *Journal of Combinatorial Theory*, 6(4):370–374, 1969.

[2] J. Arney and E. Bender. Random mappings with constraints on coalescence and number of origins. *Pacific Journal of Mathematics*, 103(2):269–294, 1982.

[3] E. Bach and A. Bridy. On the number of distinct functional graphs of affine-linear transformations over finite fields. *Linear Algebra and its Applications*, 439(5):1312–1320, 2013.

[4] J. Baek, A. Deopurkar, and K. Redfield. Points on conics modulo p. `https://www-cs.stanford.edu/~jbaek/18.821.paper3.pdf`, 2007.

[5] E. Bellah, D. Garton, E. Tannenbaum, and N. Walton. A probabilistic heuristic for counting components of functional graphs of polynomials over finite fields. *Involve, a Journal of Mathematics*, 11(1):169–179, 2017.

[6] R. L. Benedetto, D. Ghioca, B. Hutz, P. Kurlberg, T. Scanlon, and T. J. Tucker. Periods of rational maps modulo primes. *Mathematische Annalen*, pages 1–24, 2013.

[7] B. J. Birch. How the number of points of an elliptic curve over a fixed prime field varies. *Journal of the London Mathematical Society*, 1(1):57–60, 1968.

[8] J. Bober. On the randomness of modular inverse mappings, 2003.

[9] A. Bridy and D. Garton. Dynamically distinguishing polynomials. *Research in the Mathematical Sciences*, 4(1):13, 2017.

[10] C. Burnette and E. Schmutz. Representing random permutations as the product of two involutions. *Online J. Anal. Comb. No. 11*, 2016.

[11] S. Cantat. Birational permutations. *Comptes Rendus Mathematique*, 347(21-22):1289–1294, 2009.

[12] H. Capel, R. Sahadevan, and S. Rajakumar. Super integrable four-dimensional autonomous mappings. *Journal of Physics A: Mathematical and Theoretical*, 40(20):5373, 2007.

[13] F. Chen, K.-W. Wong, X. Liao, and T. Xiang. Period distribution of generalized discrete arnold cat map. *Theoretical Computer Science*, 552:13–25, 2014.

[14] W.-S. Chou and I. E. Shparlinski. On the cycle structure of repeated exponentiation modulo a prime. *Journal of Number Theory*, 107(2):345–356, 2004.

[15] L. Clozel, M. Harris, and R. Taylor. Automorphy for some l-adic lifts of automorphic mod l Galois representations. *Publications mathématiques*, 108(1):1, 2008.

[16] M. Degli Esposti, S. Graffi, and S. Isola. Classical limit of the quantized hyperbolic toral automorphisms. *Communications in Mathematical Physics*, 167(3):471–507, 1995.

[17] R. L. Devaney. Homoclinic orbits in Hamiltonian systems. *Journal of Differential Equations*, 21(2):431–438, 1976.

[18] L. E. Dickson. The analytic representation of substitutions on a power of a prime number of letters with a discussion of the linear group. *The Annals of Mathematics*, 11(1/6):65–120, 1896.

[19] B. Elspas. The theory of autonomous linear sequential networks. *IRE Transactions on Circuit Theory*, 6(1):45–60, 1959.

[20] P. Flajolet and A. M. Odlyzko. Random mapping statistics. In *Workshop on the Theory and Application of of Cryptographic Techniques*, pages 329–354. Springer, 1989.

[21] E. Flynn, B. Poonen, and E. F. Schaefer. Cycles of quadratic polynomials and rational points on a genus-two curve. *arXiv preprint math/9508211*, 1995.

[22] R. Flynn and D. Garton. Graph components and dynamics over finite fields. *International Journal of Number Theory*, 10(03):779–792, 2014.

[23] J. V. Z. Gathen. Tests for permutation polynomials. *SIAM Journal on Computing*, 20(3):591–602, 1991.

[24] C. L. Gilbert, J. D. Kolesar, C. A. Reiter, and J. D. Storey. Function digraphs of quadratic maps modulo p. *Fibonacci Quarterly*, 39(1):32–49, 2001.

[25] S. W. Golomb. Random permutations. *Bull. Amer. Math. Soc*, 70:747, 1964.

[26] V. Goncharov. Sur la distribution des cycles dans les permutations. In *Dokl. Akad. Nauk SSSR*, volume 35, pages 299–301, 1942.

[27] B. Grammaticos, R. Halburd, A. Ramani, and C. Viallet. How to detect the integrability of discrete systems. *Journal of Physics A: Mathematical and Theoretical*, 42(45):454002, 2009.

[28] M. Harris, N. Shepherd-Barron, and R. Taylor. A family of Calabi-Yau varieties and potential automorphy. *Annals of Mathematics*, pages 779–813, 2010.

[29] M. Hénon. Rates of escape from isolated clusters with an arbitrary mass distribution. *Astronomy and Astrophysics*, 2:151, 1969.

[30] J. Hietarinta, N. Joshi, and F. W. Nijhoff. *Discrete systems and integrability*, volume 54. Cambridge university press, 2016.

[31] B. Hutz and P. Ingram. On Poonen's conjecture concerning rational preperiodic points of quadratic maps. *arXiv preprint arXiv:0909.5050*, 2009.

[32] D. Jogia. *Algebraic Aspects of Integrability and Reversibility in Maps*. PhD thesis, UNSW, 2008.

[33] D. Jogia, J. A. G. Roberts, and F. Vivaldi. An algebraic geometric approach to integrable maps of the plane. *Journal of Physics A: Mathematical and General*, 39(5):1133, 2006.

[34] M. Kola and M. Ali. One-dimensional generalized Fibonacci tilings. *Physical Review B*, 41(10):7108, 1990.

[35] S. V. Konyagin, F. Luca, B. Mans, L. Mathieson, M. Sha, and I. E. Shparlinski. Functional graphs of polynomials over finite fields. *Journal of Combinatorial Theory, Series B*, 116:87–122, 2016.

[36] M. D. Kruskal. The expected number of components under a random mapping function. *The American Mathematical Monthly*, 61(6):392–397, 1954.

[37] J. C. Lagarias and E. Rains. Dynamics of a family of piecewise-linear area-preserving plane maps I. Rational rotation numbers. *Journal of Difference Equations and Applications*, 11(12):1089–1108, 2005.

[38] J. C. Lagarias and E. Rains. Dynamics of a family of piecewise-linear area-preserving plane maps II. Invariant circles. *Journal of Difference Equations and Applications*, 11(13):1137–1163, 2005.

[39] J. C. Lagarias and E. Rains. Dynamics of a family of piecewise-linear area-preserving plane maps III. Cantor set spectra. *Journal of Difference Equations and Applications*, 11(14):1205–1224, 2005.

[40] J. S. Lamb and J. A. Roberts. Time-reversal symmetry in dynamical systems: a survey. *Physica D: Nonlinear Phenomena*, 112(1):1–39, 1998.

[41] R. Lidl and G. L. Mullen. When does a polynomial over a finite field permute the elements of the field? *The American Mathematical Monthly*, 95(3):243–246, 1988.

[42] F. Luca. Diophantine equations. `https://www.math.dartmouth.edu/archive/m105f12/public_html/lucaHungary1.pdf`, 2007.

[43] M. Lugo. The cycle structure of compositions of random involutions. *arXiv preprint arXiv:0911.3604*, 2009.

[44] R. S. MacKay. *Renormalisation in area-preserving maps*, volume 6. World Scientific, 1993.

[45] A. Majewski. Julia iim 1.jpg. `https://en.wikipedia.org/wiki/File:Julia_IIM_1.jpg`, 2008. [Online, accessed September 11, 2018].

[46] R. Martins, D. Panario, and C. Qureshi. A survey on iterations of mappings over finite fields. *Combinatorics and Finite Fields*, pages 135–172, 07 2019.

[47] R. S. Martins and D. Panario. On the heuristic of approximating polynomials over finite fields by random mappings. *International Journal of Number Theory*, 12(07):1987–2016, 2016.

[48] S. Maubach. Polynomial automorphisms over finite fields. *Serdica Math. J.*, 27:343–350, 2001.

[49] K. E. Morrison. Random maps and permutations. `https://web.calpoly.edu/~kmorriso/Research/randommaps.pdf`, 1998.

[50] P. Morton. Arithmetic properties of periodic points of quadratic maps, ii. *Acta Arithmetica*, 87(2):89–102, 1998.

[51] P. Morton and J. H. Silverman. Rational periodic points of rational functions. *International Mathematics Research Notices*, 1994(2):97–110, 1994.

[52] N. Neumärker, J. A. G. Roberts, and F. Vivaldi. Distribution of periodic orbits for the Casati–Prosen map on rational lattices. *Physica D: Nonlinear Phenomena*, 241(4):360–371, 2012.

[53] D. G. Northcott. Periodic points on an algebraic variety. *Annals of Mathematics*, pages 167–177, 1950.

[54] A. Ostafe and M. Sha. Counting dynamical systems over finite fields. *Contemp. Math*, 669:187–203, 2016.

[55] I. Percival and F. Vivaldi. Arithmetical properties of strongly chaotic motions. *Physica D: Nonlinear Phenomena*, 25(1-3):105–130, 1987.

[56] J. Peyrière. On the trace map for products of matrices associated with substitutive sequences. *Journal of statistical physics*, 62(1):411–414, 1991.

[57] J. M. Pollard. A Monte Carlo method for factorization. *BIT Numerical Mathematics*, 15(3):331–334, 1975.

[58] B. Poonen. The classification of rational preperiodic points of quadratic polynomials over $\mathbb{Q}$: a refined conjecture. *Mathematische Zeitschrift*, 228(1):11–29, 1998.

[59] C. Qureshi and D. Panario. Rédei actions on finite fields and multiplication map in cyclic group. *SIAM J. Discrete Math.*, 29(3):1486–1503, 2015.

[60] J. A. G. Roberts, A. Iatrou, and G. Quispel. Interchanging parameters and integrals in dynamical systems: the mapping case. *Journal of Physics A: Mathematical and General*, 35(9):2309, 2002.

[61] J. A. G. Roberts, D. Jogia, and F. Vivaldi. The Hasse-Weil bound and integrability detection in rational maps. *Journal of Nonlinear Mathematical Physics*, 10(sup2):166–180, 2003.

[62] J. A. G. Roberts and F. Vivaldi. Arithmetical method to detect integrability in maps. *Physical review letters*, 90(3):034102, 2003.

[63] J. A. G. Roberts and F. Vivaldi. Signature of time-reversal symmetry in polynomial automorphisms over finite fields. *Nonlinearity*, 18(5):2171, 2005.

[64] J. A. G. Roberts and F. Vivaldi. A combinatorial model for reversible rational maps over finite fields. *Nonlinearity*, 22(8):1965, 2009.

[65] T. D. Rogers. The graph of the square mapping on the prime fields. *Discrete Mathematics*, 148(1-3):317–324, 1996.

[66] I. Rubio and C. Corrada-Bravo. Cyclic decomposition of permutations of finite fields obtained using monomials and applications to turbo codes. In *Proceedings of Finite Fields and Applications Symposium*, 2003.

[67] I. M. Rubio and C. J. Corrada-Bravo. Cyclic decomposition of permutations of finite fields obtained using monomials. In *Finite fields and applications*, pages 254–261. Springer, 2004.

[68] I. M. Rubio, G. L. Mullen, C. Corrada, and F. N. Castro. Dickson permutation polynomials that decompose in cycles of the same length. *Contemporary Mathematics*, 461:229–240, 2008.

[69] M. Sha. On the cycle structure of repeated exponentiation modulo a prime power. *Fibonacci Quart. 49, no. 4, 340347.*, 2011.

[70] L. Shepp and S. Lloyd. Ordered cycle lengths in a random permutation. *Transactions of the American Mathematical Society*, 121(2):340–357, 1966.

[71] I. E. Shparlinski. A deterministic test for permutation polynomials. *Computational complexity*, 2(2):129–132, 1992.

[72] Solkoll. Time escape Julia set from coordinate (phi-2, 0).jpg. `https://en.wikipedia.org/wiki/File:Time_escape_Julia_set_from_coordinate_(phi-2,_0).jpg`, 2005. [Online, accessed September 11, 2018].

[73] J. T. Tate. Algebraic cycles and poles of zeta functions. In *Arithmetical Algebraic Geometry (Proc. Conf. Purdue Univ., 1963)*, pages 93–110. Harper & Row, New York, 1965.

[74] R. Taylor. Automorphy for some l-adic lifts of automorphic mod l galois representations. ii. *Publications mathématiques*, 108(1):183–239, 2008.

[75] G. Turnwald. On Schur's conjecture. *Journal of the Australian Mathematical Society*, 58(3):312–357, 1995.

[76] T. Vasiga and J. Shallit. On the iteration of certain quadratic maps over GF (p). *Discrete Mathematics*, 277(1-3):219–240, 2004.

[77] F. Vivaldi. Geometry of linear maps over finite fields. *Nonlinearity*, 5(1):133, 1992.